

Fast-Decodable MIDO Codes with large Coding Gain

K. Pavan Srinath and B. Sundar Rajan, *Senior Member, IEEE*

Dept of ECE, The Indian Institute of Science,

Bangalore-560012, India

Email:{pavan,bsrajan}@ece.iisc.ernet.in

Abstract—In this paper, a new method is proposed to obtain full-diversity, rate-2 (rate of 2 complex symbols per channel use) space-time block codes (STBCs) that are full-rate for multiple input, double output (MIDO) systems and unlike existing full-diversity STBCs, are not obtainable as matrix representations of division algebras. Using this method, rate-2 STBCs for 4×2 , 6×2 , 8×2 and 12×2 systems are constructed and these STBCs are fast ML-decodable, have large coding gains and STBC-schemes consisting of these STBCs have a non-vanishing determinant (NVD) so that they are DMT-optimal for their respective MIDO systems. It is also shown that the Srinath-Rajan code [1, Subsection VIII-C] for the 4×2 system, which was proposed in [2] and has the lowest ML-decoding complexity among known rate-2 STBCs for the 4×2 MIDO system with a large coding gain for 4-/16-QAM, has the same algebraic structure as the STBC constructed in this paper for the 4×2 system. This also settles in positive a previous conjecture that the STBC-scheme that is based on the Srinath-Rajan code has the NVD property and hence is DMT-optimal for the 4×2 system.

Index Terms—Cyclic division algebra, fast-decodability, Galois group, MIDO system, non-vanishing determinant, space-time block code.

I. INTRODUCTION AND BACKGROUND

Space-time block coding [3] has been continually evolving over the last decade. Beginning with the simple Alamouti code [4] for 2 transmit antennas, the evolution of space-time coding theory has resulted in the development of sophisticated full-diversity codes from cyclic division algebras (CDAs) [5]-[9] for any number of transmit antennas. At one end are the rate-1 (a rate- m code transmits m complex information symbols in each channel use) STBCs that are multi-group decodable (see, for example, [10]-[13] for a definition of multi-group decodable STBCs) and have a relatively low maximum likelihood (ML)-decoding complexity while at the other end are rate- n_t (for n_t transmit antennas) full-diversity STBCs obtained from CDAs which have a very high ML-decoding complexity. The usage of powerful tools from number theory has resulted in rate- n_t (for n_t transmit antennas) STBCs with high coding gains and STBC-schemes (see Definition 2) employing these codes have a non-vanishing determinant (see Definition 3) so that they are diversity-multiplexing gain tradeoff (DMT)-optimal [8] for any number of receive antennas. Examples of such codes are the perfect codes [7], [9].

Recent interest has been towards asymmetric MIMO systems where the number of receive antennas n_r is less than the number of transmit antennas n_t . Such a scenario occurs,

for example, in the downlink transmission from a base station to a mobile phone, and in digital video broadcasting (DVB) where communication is between a TV broadcasting station and a portable TV device (see, for example, [14]). Of particular interest is the 4×2 MIDO system for which a slew of rate-2 STBCs have been developed [1], [2], [15]-[20], with the particular aim of allowing fast-decodability (See Definition 4), a term that was first coined in [15]. Among these codes, those in [1], [16]-[20] have been shown to have a minimum determinant that is bounded away from zero irrespective of the size of the signal constellation and hence STBC-schemes that consist of these codes have the NVD property and are DMT-optimal for the 4×2 MIDO system [22]. All these STBCs are either from CDAs or from crossed product algebras [16], [19]. A generalization of fast-decodable STBC construction for higher number of transmit antennas has been proposed in [1]. STBCs from non-associative division algebras have also been proposed in [21].

The best performing code for the 4×2 MIDO system is the Srinath-Rajan code [2] which has the least ML-decoding complexity (of the order of $M^{4.5}$ for a square M -QAM) among comparable codes and the best known normalized minimum determinant (see Definition 1) for 4-/16-QAM. However, this code was constructed using an ad hoc technique and had not been proven to have a non-vanishing determinant for arbitrary QAM constellations. In this paper, we propose a novel construction scheme to obtain rate-2 STBCs which have full-diversity and STBC-schemes that employ these codes have the NVD property. We then explicitly construct such STBCs for $n \times 2$ MIDO systems, $n = 4, 6, 8, 12$ and these codes are fast-decodable and have large normalized minimum determinants.

A. Contributions and paper organization

The contributions of this paper are the following.

- 1) We propose a novel method to construct rate-2 STBCs with full-diversity. These STBCs are not obtainable as matrix representations of division algebras unlike previous constructions.
- 2) Using our construction methodology, we construct rate-2, fast-decodable STBCs for 4×2 , 6×2 , 8×2 and 12×2 MIDO systems. All these four STBCs have large normalized minimum determinants and relatively lower ML-decoding complexity compared to the best known

# Tx antennas	STBC	Constellation (average energy E)	δ_{min}	ML-decoding complexity
4	$\mathcal{S}_{4 \times 2}$	QAM	$\frac{1}{25E^4}$	$M^{4.5}$
	Punctured ^{\$} perfect code [7]	QAM	$\frac{16}{1125E^4}$	$M^{5.5}$
	\mathcal{C}_1 [1], [17]	QAM	$\frac{1}{25E^4}$	$M^{6.5}$
	Punctured \mathcal{C}_4 (New)	QAM	$\frac{1}{16E^4}$	M^7
6	$\mathcal{S}_{6 \times 2}$	HEX	$\frac{1}{7^4 E^6}$	$M^{8.5}$
	Punctured perfect code [7]	HEX	$\frac{1}{7^5 E^6} \leq \delta_{min} \leq \frac{1}{7^4 E^6}$	$M^{11.5}$
	Punctured \mathcal{C}_6	HEX	$\frac{1}{(3E)^6}$	$M^{11.5}$
	VHO-Code [1]	QAM	Not available [‡]	$M^{7.5}$
8	$\mathcal{S}_{8 \times 2}$	QAM	$\frac{1}{25(15)^4 E^8}$	$M^{9.5}$
	Punctured perfect code [9]	QAM	$\frac{1}{5^7 2^{16} E^8}$	$M^{15.5}$
12	$\mathcal{S}_{12 \times 2}$	HEX	$\delta_{min} \geq \frac{1}{(14E)^{12}}$	$M^{17.5}$

^{\$} Punctured STBCs for $n_r < n_t$ refer to rate- n_r STBCs obtained from rate- n_t STBCs (which transmit n_t^2 complex symbols in n_t channel uses) by restricting the number of complex symbols transmitted to be only $n_t n_r$.

[‡] This STBC, although equipped with the NVD property, has its non-norm element $\gamma = -3/4$ which does not satisfy $|\gamma|^2 = 1$. The exact minimum determinant is hard to explicitly calculate.

TABLE I
COMPARISON OF OUR STBCS WITH KNOWN BEST STBCS.

STBCs in their class (see Table I). In addition, STBC-schemes that consist of these STBCs have the NVD property making them DMT-optimal for their respective MIDO systems.

- 3) We show that the Srinath-Rajan (SR) code [2] has the same underlying algebraic structure as the STBC constructed in this paper for the 4×2 system. This way, we prove the conjecture that the STBC-scheme based on the SR-code has the NVD property.

The paper is organized as follows. Section II gives the system model, relevant definitions and a brief overview of CDAs. Section III builds the theory needed to obtain rate-2 STBCs while Section IV deals with the construction of fast-decodable STBCs for 4×2 , 6×2 , 8×2 and 12×2 systems. The property of the constructed STBCs that allows fast-decodability is explained in Section V and simulation results are given in Section VI. Concluding remarks constitute Section VII.

Notations

Throughout the paper, the following notations are used.

- Bold, lowercase letters denote vectors and bold, upper-case letters denote matrices.
- \mathbf{X}^H , \mathbf{X}^T , $\det(\mathbf{X})$, $\text{tr}(\mathbf{X})$ and $\|\mathbf{X}\|$ denote the Hermitian, the transpose, the determinant, the trace and the Frobenius norm of \mathbf{X} , respectively.
- $\text{diag}[\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n]$ denotes a block diagonal matrix with matrices $\mathbf{A}_1, \mathbf{A}_2, \dots, \mathbf{A}_n$ on its main diagonal blocks.
- The real and the imaginary parts of a complex-valued vector \mathbf{x} are denoted by \mathbf{x}_I and \mathbf{x}_Q , respectively.
- $|\mathcal{S}|$ denotes the cardinality of the set \mathcal{S} and for set $\mathcal{T} \subset \mathcal{S}$, $\mathcal{S} \setminus \mathcal{T}$ denotes the set of elements of \mathcal{S} not in \mathcal{T} .
- \mathbf{I} and \mathbf{O} denote the identity and the null matrix of appropriate dimension.
- For a random variable X , its expectation is denoted by $\mathbb{E}(X)$.
- \mathbb{R} , \mathbb{C} and \mathbb{Q} denote the field of real, complex and rational numbers, respectively. \mathbb{Z} denotes the ring of rational integers.
- Unless used as a subscript or a superscript, i denotes $\sqrt{-1}$ and ω denotes the primitive third root of unity.
- For fields \mathbb{K} and \mathbb{F} , \mathbb{K}/\mathbb{F} denotes that \mathbb{K} is an extension

of \mathbb{F} (hence, \mathbb{K} is an algebra over \mathbb{F}) and $[\mathbb{K} : \mathbb{F}] = m$ indicates that \mathbb{K} is a finite extension of \mathbb{F} of degree m .

- $\text{Gal}(\mathbb{K}/\mathbb{F})$ denotes the Galois group of \mathbb{K}/\mathbb{F} , i.e., the group of \mathbb{F} -linear automorphisms of \mathbb{K} . If σ is any \mathbb{F} -linear automorphism of \mathbb{K} , $\langle \sigma \rangle$ denotes the cyclic group generated by σ .
- The elements 1 and 0 are understood to be the multiplicative and the additive identity elements, respectively, of the unit ring \mathcal{R} in context.

II. SYSTEM MODEL AND DEFINITIONS

We consider an n_t transmit antenna, n_r receive antenna MIMO system ($n_t \times n_r$ system) with perfect channel-state information available at the receiver (CSIR) alone. The channel is assumed to be quasi-static with Rayleigh fading. The system model is

$$\mathbf{Y} = \rho \mathbf{H} \mathbf{S} + \mathbf{N}, \quad (1)$$

where $\mathbf{Y} \in \mathbb{C}^{n_r \times T}$ is the received signal matrix, $\mathbf{S} \in \mathbb{C}^{n_t \times T}$ is the codeword matrix that is transmitted over a block of T channel uses, $\mathbf{H} \in \mathbb{C}^{n_r \times n_t}$ and $\mathbf{N} \in \mathbb{C}^{n_r \times T}$ are respectively the channel matrix and the noise matrix with entries independently and identically distributed (i.i.d.) circularly symmetric complex Gaussian random variables with zero mean and unit variance. The average signal-to-noise ratio (SNR) at each receive antenna is denoted by ρ . It follows that

$$\mathbb{E}(\|\mathbf{S}\|^2) = T. \quad (2)$$

A space-time block code (STBC) \mathcal{S} of block-length T for an n_t transmit antenna MIMO system is a finite set of complex matrices of size $n_t \times T$. An STBC transmitting k independent complex information symbols in T channel uses is said to have a rate of k/T complex symbols per channel use. An STBC having a rate of $\min(n_t, n_r)$ independent complex information symbols per channel use is said to be a full-rate STBC. Throughout the paper, we consider linear STBCs [24] encoding symbols from a complex constellation \mathcal{A}_q which is QAM or HEX. An M -PAM, M -QAM and M -HEX, with $M = 2^a$, $a > 0$, are respectively given as

$$\begin{aligned} M\text{-PAM} &= \{-M+1, -M+3, -M+5, \dots, M-1\}, \\ M\text{-QAM} &= \{a+ib, a, b \in \sqrt{M}\text{-PAM}\}, \\ M\text{-HEX} &= \{a+\omega b, a, b \in \sqrt{M}\text{-PAM}\}. \end{aligned}$$

Assuming that \mathcal{A}_q is M -QAM or M -HEX, the symbols s_i encoded by the STBC are of the form $s_i \triangleq \bar{s}_i + \beta \check{s}_i$, with $\bar{s}_i, \check{s}_i \in \sqrt{M}\text{-PAM}$ and $\beta = i$ or ω depending on whether \mathcal{A}_q is M -QAM or M -HEX, respectively (when M -QAM is used, \bar{s}_i is the same as s_{iI} and \check{s}_i is the same as s_{iQ}). Therefore, the STBC \mathcal{S} is of the form

$$\mathcal{S} = \left\{ \mathbf{S}_i = \sum_{j=1}^k (\bar{s}_{ij} \bar{\mathbf{A}}_j + \check{s}_{ij} \check{\mathbf{A}}_j) \right\} \quad (4)$$

where \mathbf{S}_i , $i = 1, 2, \dots, |\mathcal{A}_q|^k$ are the codeword matrices, the complex symbol $s_{ij} \in \mathcal{A}_q$, and $\bar{\mathbf{A}}_j$ and $\check{\mathbf{A}}_j$ are its associated complex weight matrices. We assume that the average energy of \mathcal{A}_q is E units. Noting the symmetry of

both M -QAM and M -HEX, we have $\mathbb{E}(|\bar{s}_{ij}|^2) = \mathbb{E}(|\check{s}_{ij}|^2) = E/2$, $\mathbb{E}(\bar{s}_{ij} \check{s}_{ij}) = 0$. and so, the energy constraint in (2) translates to $E \sum_{i=1}^k \text{tr}(\bar{\mathbf{A}}_i \bar{\mathbf{A}}_i^H + \check{\mathbf{A}}_i \check{\mathbf{A}}_i^H) = 2T$. We assume that $\sum_{i=1}^k \text{tr}(\bar{\mathbf{A}}_i \bar{\mathbf{A}}_i^H + \check{\mathbf{A}}_i \check{\mathbf{A}}_i^H) = 2T$ so that all codeword matrices of \mathcal{S} are normalized by a factor of $\frac{1}{\sqrt{E}}$. Among STBCs transmitting at the same rate in bits per channel use, the metric for comparison that decides their error performance is the normalized minimum determinant which is defined as follows.

Definition 1: (Normalized minimum determinant) For an STBC $\mathcal{S} = \{\mathbf{S}_i, i = 1, \dots, |\mathcal{S}|\}$ that satisfies (2), the normalized minimum determinant $\delta_{\min}(\mathcal{S})$ is defined as

$$\delta_{\min}(\mathcal{S}) = \min_{\mathbf{S}_i, \mathbf{S}_j \in \mathcal{S}, i \neq j} |\det(\mathbf{S}_i - \mathbf{S}_j)|^2. \quad (5)$$

For full-diversity STBCs, $\delta_{\min}(\mathcal{S})$ defines the coding gain [3]. Between two competing STBCs, the one with the larger normalized minimum determinant is expected to have a better error performance.

Note 1: When the average energy of transmission in each time slot is uniform, then the energy constraint given by (2) implies that $\mathbb{E}(\|\mathbf{s}_i\|^2) = 1$, $\forall i = 1, \dots, T$, where \mathbf{s}_i denotes the i^{th} column of a codeword matrix.

Definition 2: (STBC-scheme [23]) An STBC-scheme $\mathcal{X}_{\text{scheme}}$ is defined as a family of STBCs indexed by ρ , each STBC of block length T so that $\mathcal{X}_{\text{scheme}} = \{\mathcal{S}(\rho)\}$, where the STBC $\mathcal{S}(\rho)$ corresponds to a signal-to-noise ratio of ρ at each receive antenna.

For STBC-schemes that consist of linear STBCs employing complex lattice constellations, the weight matrices define the STBC-scheme. The weight matrices are fixed and the size and average energy of the signal constellation are allowed to vary in accordance with ρ . Associated with such linear STBC-schemes is the notion of non-vanishing determinant (NVD).

Definition 3: (Non-vanishing determinant [6]) A linear STBC-scheme $\mathcal{X}_{\text{scheme}}$, whose STBCs are defined by weight matrices $\{\bar{\mathbf{A}}_i, \check{\mathbf{A}}_i, i = 1, \dots, k\}$ and employ complex constellations that are finite subsets of an infinite complex lattice \mathcal{A}_L , is said to have the non-vanishing determinant (NVD) property if $\mathcal{S}_{\infty} \triangleq \left\{ \sum_{i=1}^k (\bar{s}_i \bar{\mathbf{A}}_i + \check{s}_i \check{\mathbf{A}}_i) \mid s_i \in \mathcal{A}_L \right\}$ is such that

$$\min_{\mathbf{S} \in \mathcal{S}_{\infty}, \mathbf{S} \neq \mathbf{0}} \{|\det(\mathbf{S})|^2\} = c > 0$$

for some strictly positive constant c .

With respect to ML-decoding, if the STBC transmits k complex symbols in T channel uses, where the symbols are encoded from a suitable complex constellation of size M , an exhaustive search requires performing $\mathcal{O}(M^k)$ operations ($\mathcal{O}()$ stands for “big O of”) because the k symbols have to be jointly evaluated. However, some STBCs allow fast-decodability and are defined as follows.

Definition 4: (Fast-decodable STBC [15]) Consider an STBC encoding k complex information symbols from a complex constellation of size M . If the ML-decoding of this STBC by an exhaustive search involves performing only $\mathcal{O}(M^p)$ computations, $p < k$, the STBC is said to be fast-decodable.

For more on fast-decodability, one can refer to [15], [2].

$$\mathbf{F} = \begin{bmatrix} a_0 & \gamma\tau(a_{n-1}) & \gamma\tau^2(a_{n-2}) & \cdots & \gamma\tau^{n-1}(a_1) \\ a_1 & \tau(a_0) & \gamma\tau^2(a_{n-1}) & \cdots & \gamma\tau^{n-1}(a_2) \\ a_2 & \tau(a_1) & \tau^2(a_0) & \cdots & \gamma\tau^{n-1}(a_3) \\ a_3 & \tau(a_2) & \tau^2(a_1) & \cdots & \gamma\tau^{n-1}(a_4) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{n-1} & \tau(a_{n-2}) & \tau^2(a_{n-3}) & \cdots & \tau^{n-1}(a_0) \end{bmatrix}. \quad (3)$$

A. Cyclic Division Algebras

A cyclic division algebra (CDA) \mathcal{A} of degree n over a number field \mathbb{F} is a vector space over \mathbb{F} of dimension n^2 . The center of \mathcal{A} is \mathbb{F} and there exists a maximal subfield \mathbb{K} of \mathcal{A} such that \mathbb{K} is a Galois extension of degree n over \mathbb{F} with a cyclic Galois group generated by τ . \mathcal{A} is a right vector space over \mathbb{K} and can be expressed as $\mathcal{A} = \mathbb{K} \oplus \mathbf{i}\mathbb{K} \oplus \mathbf{i}^2\mathbb{K} \oplus \cdots \oplus \mathbf{i}^{n-1}\mathbb{K}$, where $\mathbf{a}\mathbf{i} = \mathbf{i}\tau(a)$, $\forall a \in \mathbb{K}$, $\mathbf{i}^n = \gamma$, for some $\gamma \in \mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ such that the norm $N_{\mathbb{K}/\mathbb{F}}(a) = \prod_{i=0}^{n-1} \tau^i(a)$ of any element $a \in \mathbb{K}$ satisfies

$$N_{\mathbb{K}/\mathbb{F}}(a) \neq \gamma^t, \quad t = 1, \dots, n-1. \quad (6)$$

The CDA \mathcal{A} is denoted by $(\mathbb{K}/\mathbb{F}, \tau, \gamma)$. \mathcal{A} has a matrix representation and in particular, an element $a_0 + \mathbf{i}a_1 + \cdots + \mathbf{i}^{n-1}a_{n-1}$ of \mathcal{A} , where $a_i \in \mathbb{K}$, has the representation shown in (3) at the top of the page. In addition, $\det(\mathbf{F}) \in \mathbb{F}^\times$, for a nonzero \mathbf{F} [27]. For more on CDAs, one can refer to [5], [27] and references therein.

B. STBCs from CDA

In this section, we review some known techniques to obtain full-diversity STBC-schemes with a non-vanishing determinant and large coding gain. For the purpose of space time coding, the signal constellation is generally M -QAM, M -HEX or M -PAM which are finite subsets of $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ and \mathbb{Z} , respectively. So, \mathbb{F} is naturally chosen to be $\mathbb{Q}(i)$, $\mathbb{Q}(\omega)$, or simply \mathbb{Q} for which the ring of integers are respectively $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ and \mathbb{Z} . By $\mathcal{O}_{\mathbb{F}}$ and $\mathcal{O}_{\mathbb{K}}$, we denote the ring of integers of \mathbb{F} and \mathbb{K} respectively. When $[\mathbb{K} : \mathbb{F}] = n$, \mathbb{K} has an \mathbb{F} -basis of cardinality n . Similarly, $\mathcal{O}_{\mathbb{K}}$ has an $\mathcal{O}_{\mathbb{F}}$ -basis of cardinality n . An \mathbb{F} -basis $\{\theta_i, i = 1, 2, \dots, n | \theta_i \in \mathcal{O}_{\mathbb{K}}\}$ is chosen and the $a_i \in \mathbb{K}$ in (3) are expressed as linear combinations of elements of this basis over $\mathcal{O}_{\mathbb{F}}$. The STBC which encodes symbols from a complex constellation \mathcal{A}_q (M -QAM, M -HEX) is given by $\mathcal{S} = \{\mathbf{S}_i, i = 1, \dots, R\}$, where the codewords \mathbf{S}_i have the form shown in (3) with $a_i = \sum_{j=1}^n s_{ij}\theta_j$, $s_{ij} \in \mathcal{A}_q \subset \mathcal{O}_{\mathbb{F}}$ with $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[i]$, $\mathbb{Z}[\omega]$ or \mathbb{Z} . A codeword matrix of STBCs from CDA has n_t layers [7], with the $(i+1)^{th}$ layer transmitting the vector $\mathbf{D}_i[a_i, \tau(a_i), \dots, \tau^{n-1}(a_i)]^T$, $i = 0, \dots, n_t - 1$, where

$$\mathbf{D}_i \triangleq \text{diag}[\underbrace{1, \dots, 1}_{n_t-i \text{ times}}, \underbrace{\gamma, \dots, \gamma}_i].$$

The \mathbb{F} -basis $\{\theta_i, i = 1, 2, \dots, n | \theta_i \in \mathcal{O}_{\mathbb{K}}\}$ is generally chosen such that the matrix

$$\mathbf{R} = \begin{bmatrix} \theta_1 & \theta_2 & \cdots & \theta_n \\ \tau(\theta_1) & \tau(\theta_2) & \cdots & \tau(\theta_n) \\ \vdots & \vdots & \ddots & \vdots \\ \tau^{n-1}(\theta_1) & \tau^{n-1}(\theta_2) & \cdots & \tau^{n-1}(\theta_n) \end{bmatrix} \quad (7)$$

is scaled unitary, i.e., $\mathbf{R}\mathbf{R}^H = \lambda\mathbf{I}$ for some $\lambda \in \mathbb{R}$ (the scalar $1/\sqrt{\lambda}$ is the normalizing factor for \mathbf{R} to ensure that the energy constraint is satisfied). Further γ is generally chosen such that $|\gamma|^2 = 1$. The perfect codes, which employ these techniques, have among the largest known coding gains in their class.

III. GENERAL SCHEME FOR RATE-2 STBC CONSTRUCTION

We consider a non-commutative ring $\mathcal{M}_{\mathcal{A}}$ which is an n -dimensional bimodule over a division ring \mathcal{A} (i.e., both a left \mathcal{A} -module and a right \mathcal{A} -module), but we will treat $\mathcal{M}_{\mathcal{A}}$ as a right \mathcal{A} -module in this paper. The division ring \mathcal{A} is itself considered to be a finite dimensional cyclic algebra over a suitable number field \mathbb{F} . Let \mathbb{K} be the maximal subfield of \mathcal{A} with $[\mathbb{K} : \mathbb{F}] = m$ so that \mathcal{A} is m^2 -dimensional over \mathbb{F} , and m -dimensional as a right vector space over \mathbb{K} with basis $\{1, \mathbf{j}, \mathbf{j}^2, \dots, \mathbf{j}^{m-1}\}$. The elements of \mathcal{A} are of the form $a_0 + \mathbf{j}a_1 + \cdots + \mathbf{j}^{m-1}a_{m-1}$, with $a_i \in \mathbb{K}$, and

$$\begin{aligned} \mathbf{a}\mathbf{j} &= \mathbf{j}\sigma(a), \quad \forall a \in \mathbb{K}, \\ \mathbf{j}^m &= \gamma, \quad \text{for some } \gamma \in \mathbb{F}, \end{aligned}$$

where σ is the cyclic generator of $\text{Gal}(\mathbb{K}/\mathbb{F})$.

We denote the elements of the basis of $\mathcal{M}_{\mathcal{A}}$ over \mathcal{A} by $1, \mathbf{i}, \mathbf{i}^2, \dots, \mathbf{i}^{n-1}$. To explain the rules of multiplication in $\mathcal{M}_{\mathcal{A}}$, we consider \mathbb{K} as a Galois extension of degree n over a number field $\mathbb{F}_1 \neq \mathbb{F}$, with $\text{Gal}(\mathbb{K}/\mathbb{F}_1) = \langle \tau \rangle$. The elements of $\mathcal{M}_{\mathcal{A}}$ are of the form $A_0 + \mathbf{i}A_1 + \cdots + \mathbf{i}^{n-1}A_{n-1}$, with $A_i \in \mathcal{A}$ and

$$\mathbf{A}\mathbf{i} = \mathbf{i}\Upsilon(A), \quad \forall A \in \mathcal{A}, \quad (8)$$

$$\mathbf{i}^n = \gamma_M, \quad \text{for some } \gamma_M \in \mathcal{A} \quad (9)$$

where,

$$\Upsilon(A) \triangleq \tau(a_0) + \mathbf{j}\tau(a_1) + \cdots + \mathbf{j}^{m-1}\tau(a_{m-1}) \quad (10)$$

for $A = a_0 + \mathbf{j}a_1 + \cdots + \mathbf{j}^{m-1}a_{m-1}$, $a_1, \dots, a_{m-1} \in \mathbb{K}$. Noting that σ and τ commute (i.e., $\sigma\tau(a) = \tau\sigma(a)$), it follows that

$$\Upsilon(A)\Upsilon(B) = \Upsilon(AB), \quad A, B \in \mathcal{A}. \quad (11)$$

Now, forcing the relation $\mathbf{i}^a\mathbf{i}^b = \mathbf{i}^{a+b}$ for positive integral values of a and b , (9) implies that $\gamma_M\mathbf{i} = \mathbf{i}\gamma_M$ so that γ_M is invariant under Υ . Hence, it follows that γ_M is of the form $a_0 + \mathbf{j}a_1 + \cdots + \mathbf{j}^{m-1}a_{m-1}$, $a_i \in \mathbb{F}_1$, $i = 0, 1, \dots, m-1$. In this paper, we only consider the case where $\gamma_M \in \mathbb{F}_1 \subset \mathbb{K}$.

Example 1: Consider \mathcal{A} to be $(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(\sqrt{2}), \sigma : i \mapsto -i, -1)$ which is known to be a division algebra and is a subalgebra of Hamilton's quaternion. Next consider the Galois extension $\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(i)$ whose Galois group is $\{1, \tau\}$ with $\tau : \sqrt{2} \rightarrow -\sqrt{2}$. Now, $\mathcal{M}_{\mathcal{A}} = \{A_0 + \mathbf{i}A_1 | A_0, A_1 \in \mathcal{A}, \mathbf{i}^2 = i\}$. If $A = a_0 + \sqrt{2}a_1 + i(a_2 + \sqrt{2}a_3) +$

$\mathbf{j}(b_0 + \sqrt{2}b_1 + i(b_2 + \sqrt{2}b_3))$ with $a_i, b_i \in \mathbb{Q}$, then $\Upsilon(A) = a_0 - \sqrt{2}a_1 + i(a_2 - \sqrt{2}a_3) + \mathbf{j}(b_0 - \sqrt{2}b_1 + i(b_2 - \sqrt{2}b_3))$.

In \mathcal{M}_A , we seek conditions under which elements of the form $A_0 + \mathbf{i}A_1$ have right inverse, i.e., for every element of the form $A_0 + \mathbf{i}A_1$, $A_0, A_1 \in \mathcal{A}$, there exists a *unique* element $B \in \mathcal{M}_A$ such that $(A_0 + \mathbf{i}A_1)B = 1$. Towards this end, we make use of the following lemma.

Lemma 1: A nonzero element A of \mathcal{M}_A has a unique right inverse if and only if it is not a left zero divisor, i.e., there exists no nonzero element $B \in \mathcal{M}_A$ such that $AB = 0$.

Proof: Obtaining a right inverse $B = B_0 + \mathbf{i}B_1 + \dots + \mathbf{i}^{n-1}B_{n-1}$, $B_i \in \mathcal{A}$, is easy and is achieved by writing A as a linear combination of elements of the basis $\{1, \mathbf{i}, \dots, \mathbf{i}^{n-1}\}$ over \mathcal{A} and the unknown variables $B_i \in \mathcal{A}$, $i = 0, 1, \dots, n-1$ are obtained by equating AB with 1. If A is not a left zero divisor, the uniqueness of the inverse follows (for if $AB = 1$ and $AB' = 1$, then $A(B - B') = 0 \Rightarrow B = B'$). Conversely, if A has a unique right inverse, it is not a left zero divisor, for if $AB = 1$ and $AC = 0$ for some $C \in \mathcal{A}$, then $A(B - C) = 1 \Rightarrow C = 0$. ■

In the following theorem, we establish conditions under which elements of \mathcal{M}_A of the form $A_0 + \mathbf{i}A_1$, $A_0, A_1 \in \mathcal{A}$ have unique right inverses.

Theorem 1: Any nonzero element of \mathcal{M}_A of the form $A_0 + \mathbf{i}A_1$, $A_0, A_1 \in \mathcal{A}$ has a unique right inverse if and only if

$$C\Upsilon(C)\Upsilon^2(C) \dots \Upsilon^{n-1}(C) \neq \gamma_M \text{ for every } C \in \mathcal{A}. \quad (12)$$

Proof: From Lemma 1, we know that $A_0 + \mathbf{i}A_1$ has a unique right inverse if and only if it is not a left zero divisor. We suppose that $A_0 + \mathbf{i}A_1$ is a left zero divisor of an element $B_0 + \mathbf{i}B_1 + \dots + \mathbf{i}^{n-1}B_{n-1}$, $B_i \in \mathcal{A}$. Since A_0 and A_1 are from \mathcal{A} which is a CDA, we can assume that neither of A_0 and A_1 is zero since otherwise the inverse always exists. Now, from our assumption,

$$(A_0 + \mathbf{i}A_1)(B_0 + \mathbf{i}B_1 + \dots + \mathbf{i}^{n-1}B_{n-1}) = 0.$$

So, noting that A_1 is invertible with its right inverse denoted by A_1^{-1} (also its left inverse as elements of a CDA have the same left and right inverses), we have

$$(A'_0 + \mathbf{i})(B'_0 + \mathbf{i}B'_1 + \dots + \mathbf{i}^{n-1}B'_{n-1}) = 0$$

where $A'_0 = A_0A_1^{-1}$, $B'_i = \Upsilon^i(A_1)B_i$, $i = 0, 1, \dots, n-1$. Due to the linear independence of $1, \mathbf{i}, \dots, \mathbf{i}^{n-1}$ over \mathcal{A} , we have

$$A'_0B'_0 + \gamma_M B'_{n-1} = 0, \quad (13)$$

$$B'_{k-1} + \Upsilon^k(A'_0)B'_k = 0, \quad k = 1, \dots, n-1. \quad (14)$$

From (13), (14) and the fact that $A'_0 \neq 0$, it is clear that $B'_i \neq 0$, $i = 0, 1, \dots, n-1$. Solving (14), we arrive at $B'_0 = (-1)^{n-1}\Upsilon(A'_0)\Upsilon^2(A'_0) \dots \Upsilon^{n-1}(A'_0)B'_{n-1}$ using which in (13), we obtain

$$[(-1)^{n-1}A'_0\Upsilon(A'_0)\Upsilon^2(A'_0) \dots \Upsilon^{n-1}(A'_0) + \gamma_M]B'_{n-1} = 0.$$

Since $B'_{n-1} \neq 0$, we have $A'_0\Upsilon(A'_0)\Upsilon^2(A'_0) \dots \Upsilon^{n-1}(A'_0) = (-1)^n\gamma_M$. Taking $-A'_0 = C$, we have

$$C\Upsilon(C)\Upsilon^2(C) \dots \Upsilon^{n-1}(C) = \gamma_M. \quad (15)$$

So, elements of the form $A_0 + \mathbf{i}A_1$ are left zero divisors if and only if (15) is satisfied. Therefore, if no $C \in \mathcal{A}$ satisfies (15), any element of the form $A_0 + \mathbf{i}A_1$ has a unique right inverse which can be computed by equating the left hand side of (13) with 1. The resulting right inverse is obtained to be $B = B_0 + \mathbf{i}B_1 + \dots + \mathbf{i}^{n-1}B_{n-1}$, where

$$B_i = [\Upsilon^i(A_1)]^{-1}B'_i, \quad i = 0, 1, \dots, n-1, \quad (16)$$

$$B'_{n-1} = \left[(-1)^{n-1} \prod_{i=0}^{n-1} \Upsilon^i(A'_0) + \gamma_M \right]^{-1}, \quad (17)$$

$$B'_{n-k} = (-1)^{k-1} \left(\prod_{i=n-k+1}^{n-1} \Upsilon^i(A'_0) \right) B'_{n-1} \quad (18)$$

and $A'_0 = A_0A_1^{-1}$. This completes the proof of the theorem. ■

Remark 1: The condition in (12) is also necessary and sufficient for any element of the form $\mathbf{i}^k A_0 + \mathbf{i}^l A_1$, $A_0, A_1 \in \mathcal{A}$, $0 \leq k < l \leq n-1$, to have a unique right inverse. The proof is on similar lines to the proof of Theorem 1.

Note that the requirement in (12) implies that $c\tau(c)\tau^2(c) \dots \tau^{n-1}(c) \neq \gamma_M$ for every $c \in \mathbb{K}$, since $\mathbb{K} \subset \mathcal{A}$. In addition, if $c\tau(c)\tau^2(c) \dots \tau^{n-1}(c) \neq \gamma_M^t$ for every $c \in \mathbb{K}$, $t = 1, \dots, n-1$, then, together with the rules specified in (8)-(10), it is clear that \mathcal{M}_A contains another cyclic division algebra $A_1 = (\mathbb{K}/\mathbb{F}_1, \tau, \gamma_M)$ whose maximal subfield is \mathbb{K} , centre \mathbb{F}_1 and basis (as a right vector space over \mathbb{K}) $\{1, \mathbf{i}, \dots, \mathbf{i}^{n-1}\}$, with $a\mathbf{i} = \mathbf{i}\tau(a)$, $\forall a \in \mathbb{K}$, $\mathbf{i}^n = \gamma_M$, for some $\gamma_M \in \mathbb{F}_1^\times$. It is to be noted from (8) that $\mathbf{i}\mathbf{j} = \mathbf{j}\mathbf{i}$. So, we have the following possibilities for γ_M and γ (recall that $\gamma = \mathbf{j}^n \in \mathbb{F}^\times$).

Case 1: $\gamma_M, \gamma \in \mathbb{F}_1 \cap \mathbb{F}$. In this case \mathcal{M}_A is actually an associative algebra over $\mathbb{F}_1 \cap \mathbb{F}$. Also, if $|Gal(\mathbb{K}/(\mathbb{F}_1 \cap \mathbb{F}))| = mn$, then \mathcal{M}_A is a crossed product algebra over $\mathbb{F}_1 \cap \mathbb{F}$. The special case of $n = 2$, $\mathbb{F}_1 = \mathbb{F}$ (so that $\sigma = \tau$) is considered in [20] to obtain full-diversity STBCs with fast-decodability for the 4×2 system.

Case 2: At least one of γ_M and γ does not belong to $\mathbb{F}_1 \cap \mathbb{F}$. In this case, \mathcal{M}_A is never an associative algebra over $\mathbb{F}_1 \cap \mathbb{F}$ and hence does not have a matrix representation, for if \mathcal{M}_A is an associative algebra over $\mathbb{F}_1 \cap \mathbb{F}$ with $\gamma_M \notin \mathbb{F}_1 \cap \mathbb{F}$, then we have $\mathbf{j}\mathbf{i}^n = \mathbf{i}^n\mathbf{j}$ due to commutativity of \mathbf{i} and \mathbf{j} , but $(\mathbf{j}\mathbf{i})\mathbf{i}^{n-1} = \mathbf{j}(\mathbf{i}\mathbf{i}^{n-1}) = \mathbf{j}\mathbf{i}^n = \mathbf{j}\gamma_M \neq \gamma_M\mathbf{j} = \mathbf{i}^n\mathbf{j}$, leading to a contradiction.

Remark 2: In [20], an interesting case of $\langle \sigma \rangle = Gal(\mathbb{K}/\mathbb{F})$, $\langle \tau \rangle = \{1, \tau\} = Gal(\mathbb{F}/\mathbb{F}_1)$, with $\mathbb{F}_1 \subset \mathbb{C} \subset \mathbb{K}$ and $\gamma_M \in \mathbb{F}$, $\gamma \in \mathbb{F}_1$ is also considered to obtain fast-decodable STBCs for the 6×3 MIMO system.

In this paper, we consider the case $\gamma_M \in \mathbb{F}_1 \setminus (\mathbb{F}_1 \cap \mathbb{F})$, $\gamma \in \mathbb{F}_1 \cap \mathbb{F}$. As an assertion of the fact that \mathcal{M}_A is not an associative algebra, it can be checked that the left inverse and the right inverse of an element of \mathcal{M}_A of the form $A_0 + \mathbf{i}A_1$, when they exist, are not the same, indicating that \mathcal{M}_A does not have a matrix representation. However, we still can make use of Theorem 1 to obtain invertible matrices, which are desirable from the point of view of constructing full-diversity STBCs.

$$\mathbf{M} = \begin{bmatrix} \mathbf{B}_0 & \gamma_M \Upsilon(\mathbf{B}_{n-1}) & \gamma_M \Upsilon^2(\mathbf{B}_{n-2}) & \cdots & \gamma_M \Upsilon^{n-1}(\mathbf{B}_1) \\ \mathbf{B}_1 & \Upsilon(\mathbf{B}_0) & \gamma_M \Upsilon^2(\mathbf{B}_{n-1}) & \cdots & \gamma_M \Upsilon^{n-1}(\mathbf{B}_2) \\ \mathbf{B}_2 & \Upsilon(\mathbf{B}_1) & \Upsilon^2(\mathbf{B}_0) & \cdots & \gamma_M \Upsilon^{n-1}(\mathbf{B}_3) \\ \mathbf{B}_3 & \Upsilon(\mathbf{B}_2) & \Upsilon^2(\mathbf{B}_1) & \cdots & \gamma_M \Upsilon^{n-1}(\mathbf{B}_4) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{B}_{n-1} & \Upsilon(\mathbf{B}_{n-2}) & \Upsilon^2(\mathbf{B}_{n-3}) & \cdots & \Upsilon^{n-1}(\mathbf{B}_0) \end{bmatrix} \quad (19)$$

In this direction, we arrive at the following result.

Lemma 2: If every element C of a cyclic division algebra \mathcal{A} of degree n is such that $C\Upsilon(C)\Upsilon^2(C)\cdots\Upsilon^{n-1}(C) \neq \gamma_M$ where γ_M is some nonzero field element of \mathcal{A} , then the matrix $C\Upsilon(C)\Upsilon^2(C)\cdots\Upsilon^{n-1}(C) - \gamma_M \mathbf{I}$ is invertible, where \mathbf{C} , $\Upsilon(\mathbf{C})$, \dots , $\Upsilon^{n-2}(\mathbf{C})$ and $\Upsilon^{n-1}(\mathbf{C})$ are respectively the matrix representations¹ of C , $\Upsilon(C)$, \dots , $\Upsilon^{n-2}(C)$ and $\Upsilon^{n-1}(C)$.

Proof: For convenience, we denote $C\Upsilon(C)\Upsilon^2(C)\cdots\Upsilon^{n-1}(C)$ by \mathbf{N}_C . We first note that $\mathbf{N}_C - \gamma_M \mathbf{I}$ is not invertible if and only if γ_M is an eigenvalue of \mathbf{N}_C . This is because if γ_M is indeed an eigenvalue of \mathbf{N}_C , then $\mathbf{N}_C \mathbf{x} = \gamma_M \mathbf{x}$ so that $\mathbf{N}_C - \gamma_M \mathbf{I}$ is not full-ranked. Conversely, if $\mathbf{N}_C - \gamma_M \mathbf{I}$ is not full-ranked, we have γ_M to be one of its eigenvalues. We now proceed to prove that γ_M is not an eigenvalue of \mathbf{N}_C when $C\Upsilon(C)\Upsilon^2(C)\cdots\Upsilon^{n-1}(C) \triangleq \mathbf{N}_C \neq \gamma_M$ for any $C \in \mathcal{A}$.

Suppose that γ_M is an eigenvalue of \mathbf{N}_C . We first establish that the eigenvector of \mathbf{N}_C associated with γ_M has entries² in \mathbb{K} . Since γ_M is an element of the maximal subfield \mathbb{K} , the entries of the rank-deficient matrix $\mathbf{N}_C - \gamma_M \mathbf{I}$ are all elements of \mathbb{K} . Hence, $\mathbf{N}_C - \gamma_M \mathbf{I}$ can be viewed as the matrix of a linear transformation from the n -dimensional vector space $\mathbb{K}^{n \times 1}$ (over \mathbb{K}) to itself, with the kernel of the transformation being nontrivial and consisting of the eigenvectors of \mathbf{N}_C associated with γ_M . We choose one such eigenvector and denote it by \mathbf{e} . So, we have

$$\mathbf{N}_C \mathbf{e} = \gamma_M \mathbf{e}. \quad (20)$$

Now, we note that \mathbf{N}_C is also obtained by left regular representation [27], as the matrix of the linear transformation $\lambda_{\mathbf{N}_C} : \mathcal{A} \rightarrow \mathcal{A}$, with $\lambda_{\mathbf{N}_C}(K) = N_C K$, $\forall K \in \mathcal{A}$. Observing that any element of \mathcal{A} can be expressed as $[1, \mathbf{j}, \dots, \mathbf{j}^{n-1}] \mathbf{k}$, $\mathbf{k} \in \mathbb{K}^{n \times 1}$, let $E = [1, \mathbf{j}, \dots, \mathbf{j}^{n-1}] \mathbf{e}$, with \mathbf{e} defined in (20). So,

$$\lambda_{\mathbf{N}_C}(E) = N_C E = [1, \mathbf{j}, \dots, \mathbf{j}^{n-1}] \mathbf{N}_C \mathbf{e} \quad (21)$$

$$= [1, \mathbf{j}, \dots, \mathbf{j}^{n-1}] \gamma_M \mathbf{e} \quad (22)$$

$$= E \gamma_M, \quad (23)$$

where (21) is by definition of left regular representation, (22) is due to (20), and (23) follows by noting that γ_M is an element of \mathbb{K} . Hence, $E^{-1} N_C E = \gamma_M$. Since we have denoted

$C\Upsilon(C)\Upsilon^2(C)\cdots\Upsilon^{n-1}(C)$ by \mathbf{N}_C , we have

$$\begin{aligned} \gamma_M &= E^{-1} C \Upsilon(C) \Upsilon^2(C) \cdots \Upsilon^{n-1}(C) E \\ &= E^{-1} C \left(\Upsilon(E) (\Upsilon(E))^{-1} \right) \Upsilon(C) \\ &\quad \times \left(\Upsilon^2(E) (\Upsilon^2(E))^{-1} \right) \Upsilon^2(C) \\ &\quad \times \cdots \left(\Upsilon^{n-1}(E) (\Upsilon^{n-1}(E))^{-1} \right) \Upsilon^{n-1}(C) E \\ &= C' \Upsilon(C') \Upsilon^2(C') \cdots \Upsilon^{n-1}(C'), \end{aligned} \quad (24)$$

where $C' \triangleq E^{-1} C \Upsilon(E)$ and (24) is obtained using (10) and (11) and also noting that $(\Upsilon(E))^{-1} = \Upsilon(E^{-1})$ (since $\Upsilon(E)\Upsilon(E^{-1}) = \Upsilon(EE^{-1}) = 1$). But (24) leads to a contradiction since there exists no $C \in \mathcal{A}$ such that $C\Upsilon(C)\Upsilon^2(C)\cdots\Upsilon^{n-1}(C) = \gamma_M$. Therefore, γ_M is never an eigenvalue of $C\Upsilon(C)\Upsilon^2(C)\cdots\Upsilon^{n-1}(C)$, which proves the lemma. ■

Let \mathcal{A}_{mat} be the ring of $m \times m$ sized invertible matrices that are representations of elements of \mathcal{A} , i.e.,

$$\mathcal{A}_{mat} = \{\mathbf{A} | \mathbf{A} \text{ is the matrix representation of } A \in \mathcal{A}\}.$$

We have already assumed that γ_M does not belong to the centre of \mathcal{A} and so does not commute with every element of \mathcal{A} because of which $\mathcal{M}_{\mathcal{A}}$ does not have a matrix representation. But every element of \mathcal{A}_{mat} commutes with $\gamma_M \mathbf{I}$ (which is not the matrix representation of γ_M and does not belong to \mathcal{A}_{mat}). For any finite or infinite set \mathcal{P} of $m \times m$ sized matrices, we use the notation $\mathcal{A}_{mat}[\mathcal{P}]$ to denote the ring of $m \times m$ matrices generated by \mathcal{P} over \mathcal{A}_{mat} . We now consider the ring $\mathcal{A}_{mat}[\gamma_M \mathbf{I}]$ which is not a division ring (for example, if Γ_M denotes the matrix representation of γ_M , then $\Gamma_M - \gamma_M \mathbf{I}$ is not invertible). Let $\mathcal{A}_{inv-mat}[\gamma_M \mathbf{I}] = \{\mathbf{B} | \mathbf{B}^{-1} \in \mathcal{A}_{mat}[\gamma_M \mathbf{I}]\}$, i.e., the set of inverses of all invertible matrices in $\mathcal{A}_{mat}[\gamma_M \mathbf{I}]$. Next, consider the infinite ring of matrices \mathcal{M} whose elements are of the form shown in (19) at the top of the page, with $\mathbf{B}_i \in \mathcal{A}_{mat}[\{\gamma_M \mathbf{I}\} \cup \mathcal{A}_{inv-mat}[\gamma_M \mathbf{I}]]$, $i = 0, \dots, n-1$. With these facts developed, we make use of Lemma 2 to obtain the following result.

Theorem 2: Let $\mathcal{M}_{\mathcal{A}}$ be such that any element of the form $A_0 + \mathbf{i}A_1$ has a unique right inverse and let \mathbf{A}_0 and \mathbf{A}_1 be matrix representations of A_0 and A_1 , respectively. Consider the matrix

$$\mathbf{M} = \begin{bmatrix} \mathbf{A}_0 & \mathbf{O} & \mathbf{O} & \cdots & \gamma_M \Upsilon^{n-1}(\mathbf{A}_1) \\ \mathbf{A}_1 & \Upsilon(\mathbf{A}_0) & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \Upsilon(\mathbf{A}_1) & \Upsilon^2(\mathbf{A}_0) & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \Upsilon^2(\mathbf{A}_1) & \cdots & \mathbf{O} \\ \vdots & \vdots & \cdots & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \cdots & \Upsilon^{n-1}(\mathbf{A}_0) \end{bmatrix}. \quad (25)$$

Then,

¹Throughout the paper we denote by $\Upsilon(\mathbf{C})$ the matrix obtained by applying τ to each entry of \mathbf{C} and for the special case of \mathbf{C} being the matrix representation of $C \in \mathcal{A}$, $\Upsilon(\mathbf{C})$ happens to be the matrix representation of $\Upsilon(C)$.

²In general, for any square matrix with entries from a field \mathbb{K} , its eigenvalues and the entries of the associated eigenvectors need not be in \mathbb{K} , but will be in the algebraic closure of \mathbb{K} .

- 1) \mathbf{M} is invertible.
- 2) $\det(\mathbf{M}) \in \mathbb{F}_1$.

Proof: 1) Let $B = B_0 + \mathbf{i}B_1 + \dots + \mathbf{i}^{n-1}B_{n-1}$ be the unique right inverse of $A_0 + \mathbf{i}A_1$ given by (16) - (18), with $A_0, A_1, B_0, \dots, B_{n-1} \in \mathcal{A}$. Let

$$\mathbf{A}'_0 \triangleq \mathbf{A}_0 \mathbf{A}_1^{-1}, \quad (26)$$

$$\mathbf{B}'_{n-1} \triangleq \left[(-1)^{n-1} \prod_{i=0}^{n-1} \Upsilon^i(\mathbf{A}'_0) + \gamma_M \mathbf{I} \right]^{-1}, \quad (27)$$

$$\mathbf{B}'_{n-k} \triangleq (-1)^{k-1} \left(\prod_{i=n-k+1}^{n-1} \Upsilon^i(\mathbf{A}'_0) \right) \mathbf{B}'_{n-1}, \quad (28)$$

$$\mathbf{B}_i \triangleq [\Upsilon^i(\mathbf{A}_1)]^{-1} \mathbf{B}'_i, \quad i = 0, 1, \dots, n-1. \quad (29)$$

The existence of \mathbf{B}'_{n-1} can be verified by applying Theorem 1 and Lemma 2 in that order. The inverse of \mathbf{M} has the form shown in (19) with \mathbf{B}_i obtained using (26)-(29). To check that this matrix, denoted by \mathbf{M}_{inv} , is indeed the inverse of \mathbf{M} , note that both \mathbf{M} and \mathbf{M}_{inv} belong to \mathcal{M} and hence their product also is in \mathcal{M} . So, it only suffices to check that the first column of the product of \mathbf{M} and \mathbf{M}_{inv} is $[1, 0, 0, \dots, 0]^T$, which follows by using (26)-(29).

2) It can be noted that $\mathbf{M} \in \mathbb{K}^{nm \times nm}$ so that $\det(\mathbf{M}) \in \mathbb{K}$. Also, $\tau^i(\det(\mathbf{M})) = \det(\Upsilon^i(\mathbf{M}))$ where, as mentioned before, $\Upsilon^i(\mathbf{M})$ refers to the matrix obtained by applying τ^i to each entry of \mathbf{M} , $i = 0, 1, \dots, n-1$. To prove that $\det(\mathbf{M}) \in \mathbb{F}_1$, it suffices to show that $\det(\Upsilon(\mathbf{M})) = \det(\mathbf{M})$, since the only elements fixed by $\text{Gal}(\mathbb{K}/\mathbb{F}_1) = \langle \tau \rangle$ are the elements of \mathbb{F}_1 . Let $\mathbf{P}(i, j)$ denote the $(i, j)^{th}$ entry of a matrix \mathbf{P} . Consider permutation matrices \mathbf{P}_1 and \mathbf{P}_2 whose nonzero elements are

$$\begin{aligned} \mathbf{P}_1(k, (n-1)m + k) &= 1, \quad k = 1, 2, \dots, m, \\ \mathbf{P}_1(k, k-m) &= 1, \quad k = m+1, m+2, \dots, nm, \\ \mathbf{P}_2(k, m+k) &= 1, \quad k = 1, 2, \dots, (n-1)m, \\ \mathbf{P}_2(k, k-(n-1)m) &= 1, \quad k = (n-1)m+1, \dots, nm. \end{aligned}$$

Now, $\mathbf{P}_1 \Upsilon(\mathbf{M}) \mathbf{P}_2$ has the following structure.

$$\begin{bmatrix} \mathbf{A}_0 & \mathbf{O} & \dots & \mathbf{O} & \dots & \Upsilon^{n-1}(\mathbf{A}_1) \\ \gamma_M \mathbf{A}_1 & \Upsilon(\mathbf{A}_0) & \dots & \mathbf{O} & \dots & \mathbf{O} \\ \mathbf{O} & \Upsilon(\mathbf{A}_1) & \dots & \vdots & \dots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \dots & \Upsilon^{i-1}(\mathbf{A}_0) & \dots & \mathbf{O} \\ \vdots & \vdots & \dots & \Upsilon^{i-1}(\mathbf{A}_1) & \dots & \mathbf{O} \\ \vdots & \vdots & \vdots & \dots & \dots & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \dots & \mathbf{O} & \dots & \Upsilon^{n-1}(\mathbf{A}_0) \end{bmatrix}. \quad (31)$$

Therefore, with diagonal matrices \mathbf{G}_1 and \mathbf{G}_2 whose nonzero diagonal elements are defined as

$$\begin{aligned} \mathbf{G}_1(k, k) &= \gamma_M, \quad k = 1, 2, \dots, m, \\ \mathbf{G}_1(k, k) &= 1, \quad k = m+1, \dots, nm, \\ \mathbf{G}_2(k, k) &= \gamma_M^{-1}, \quad k = 1, 2, \dots, m, \\ \mathbf{G}_2(k, k) &= 1, \quad k = m+1, \dots, nm, \end{aligned}$$

we observe that $\mathbf{M} = \mathbf{G}_1 \mathbf{P}_1 \Upsilon(\mathbf{M}) \mathbf{P}_2 \mathbf{G}_2$ so that $\det(\mathbf{M}) =$

$\det(\Upsilon(\mathbf{M}))$ (for $\det(\mathbf{G}_1)\det(\mathbf{G}_2) = 1$ and \mathbf{P}_1 and \mathbf{P}_2 are permutation matrices). Therefore $\det(\mathbf{M}) \in \mathbb{F}_1$. ■

Corollary 1: If all the elements of \mathbf{M} are from $\mathcal{O}_{\mathbb{K}}$, the ring of integers of \mathbb{K} , then $\det(\mathbf{M}) \in \mathbb{F}_1 \cap \mathcal{O}_{\mathbb{K}} = \mathcal{O}_{\mathbb{F}_1}$.

IV. STBC CONSTRUCTION

A. General design procedure

The general scheme to obtain invertible matrices as code-words of an STBC for nm transmit antennas are as follows.

- 1) \mathbb{F}_1 is chosen to be either $\mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$ the reason being that a finite subset of $\mathbb{Z}[i]$ is the QAM constellation and that of $\mathbb{Z}[\omega]$ is the HEX constellation, both of practical significance.
- 2) A cyclic division algebra \mathcal{A}_1 of degree n over \mathbb{F}_1 is chosen with a maximal subfield \mathbb{K} so that $\mathcal{A}_1 = (\mathbb{K}/\mathbb{F}_1, \tau, \gamma_M)$.
- 3) Another cyclic division algebra $\mathcal{A} = (\mathbb{K}/\mathbb{F}, \sigma, \gamma)$ with $\mathbb{F} \neq \mathbb{F}_1$ is chosen such that
 - a) the non-norm element γ_M of \mathcal{A}_1 does not belong to \mathbb{F} .
 - b) there exists no element $C \in \mathcal{A}$ such that $\prod_{i=0}^{n-1} \Upsilon^i(C) = \gamma_M$.

When \mathcal{A} satisfies the above conditions, any nonzero matrix having the structure shown in (25) is invertible, with \mathbf{A}_0 and \mathbf{A}_1 being matrix representations of elements A_0 and A_1 of \mathcal{A} . If \mathcal{A} is of degree m over \mathbb{F} so that $[\mathbb{K} : \mathbb{F}] = m$, then $\mathbf{A}_0, \mathbf{A}_1 \in \mathbb{K}^{m \times m}$ and so, $\mathbf{M} \in \mathbb{K}^{nm \times nm}$. Each entry of \mathbf{A}_0 and \mathbf{A}_1 which belongs to \mathbb{K} can be viewed as a linear combination of n independent elements over \mathbb{F}_1 (since $[\mathbb{K} : \mathbb{F}_1] = n$). We express each element of \mathbf{A}_0 and \mathbf{A}_1 as a linear combination of some chosen \mathbb{F}_1 -basis $\{\theta_i, i = 1, \dots, n | \theta_i \in \mathcal{O}_{\mathbb{K}}\}$ over $\mathcal{O}_{\mathbb{F}_1}$. From the point of view of space time coding, each codeword matrix of the STBC constructed using the proposed method has the structure shown in (25), where \mathbf{A}_0 specifically has the structure given in (30) at the top of the next page, with s_{ki} , $i = 1, \dots, n$, $k = 1, \dots, m$, being the complex information symbols taking values from QAM (a finite subset of $\mathbb{Z}[i]$) or HEX (a finite subset of $\mathbb{Z}[\omega]$) constellations. \mathbf{A}_1 also has the structure given in (30) and encodes another set of nm complex information symbols.

Proposition 1: The rate of the STBC whose codeword matrices have the structure given in (25) is 2 complex symbols per channel use.

Proof: The STBC encodes $2nm$ independent complex symbols in nm channel uses hence allowing a rate of 2 complex symbols per channel use. ■

Proposition 2: The minimum determinant of the STBC (unnormalized with respect to SNR) is at least 1.

Proof: With $\mathbb{F}_1 = \mathbb{Q}(i)$ or $\mathbb{Q}(\omega)$, the ring of integers in \mathbb{F}_1 is either $\mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$. Application of Corollary 1 establishes that the determinant of any nonzero codeword difference matrix of the STBC lies in $\mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$. The result of the proposition follows. ■

While our proposed scheme can be applied to a wide range of MIMO configurations, we illustrate its application to 4

$$\mathbf{A}_0 = \begin{bmatrix} \sum_{i=1}^n s_{1i}\theta_i & \gamma\sigma(\sum_{i=1}^n s_{mi}\theta_i) & \cdots & \gamma\sigma^{m-1}(\sum_{i=1}^n s_{2i}\theta_i) \\ \sum_{i=1}^n s_{2i}\theta_i & \sigma(\sum_{i=1}^n s_{1i}\theta_i) & \cdots & \gamma\sigma^{m-1}(\sum_{i=1}^n s_{3i}\theta_i) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{i=1}^n s_{mi}\theta_i & \sigma(\sum_{i=1}^n s_{(m-1)i}\theta_i) & \cdots & \sigma^{m-1}(\sum_{i=1}^n s_{1i}\theta_i) \end{bmatrix}. \quad (30)$$

MIDO configurations³ - 4×2 , 6×2 , 8×2 and 12×2 systems. The reason for choosing these 4 configurations is easy to see - the existence of perfect codes [7] for 2, 4, 6, 8 transmit antennas and the Alamouti code for 2 transmit antennas. The perfect codes of [7] are known for their large coding gain while the Alamouti code has the least ML-decoding complexity among STBCs from CDAs in addition to having the best coding gain among known rate-1 codes for the 2×1 system. We wish to combine the advantages of both these STBCs and so, we focus on the four mentioned MIDO systems. We choose \mathcal{A} to be a subalgebra of the Alamouti algebra $\mathcal{A}_{Ala} = (\mathbb{C}/\mathbb{R}, \sigma, -1) = \{a + \mathbf{j}b, a, b \in \mathbb{C}, \mathbf{j}^2 = -1, a\mathbf{j} = \mathbf{j}\sigma(a), \forall a \in \mathbb{C}\}$ which is a cyclic division algebra over \mathbb{R} and hence a division algebra over any subfield of \mathbb{R} . The Galois group of \mathbb{C}/\mathbb{R} is $\{1, \sigma\}$ where $\sigma : i \mapsto -i$. The subalgebra that we choose is of the form $\mathcal{A} = (\mathbb{K}/\mathbb{F}, \sigma, -1)$ which is an algebra over a real number field \mathbb{F} and $\mathbb{K} = \mathbb{F}(i)$ or $\mathbb{F}(\omega)$, depending on the MIDO configuration. The code construction is illustrated in the following subsections.

B. 4×2 MIDO system

We choose \mathcal{A}_1 to be the Golden algebra over $\mathbb{Q}(i)$ given by $\mathcal{A}_1 = \{a + \mathbf{i}b, a, b \in \mathbb{Q}(i, \sqrt{5}), \mathbf{i}^2 = i, a\mathbf{i} = a\tau(a), \forall a \in \mathbb{Q}(i, \sqrt{5})\}$. The Galois group of $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$ is $\{1, \tau\}$, where $\tau(\sqrt{5}) = -\sqrt{5}$. \mathcal{A} is chosen to be a subalgebra of the Alamouti algebra with $\mathbb{F} = \mathbb{Q}(\sqrt{5})$, i.e., $\mathcal{A} = (\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(\sqrt{5}), \sigma, -1)$. Note that $\gamma_M = i \notin \mathbb{Q}(\sqrt{5})$. The STBC (unnormalized with respect to SNR) is given by

$$\mathcal{S}_{4 \times 2} = \left\{ \begin{bmatrix} a_0 & -\sigma(a_1) & i\tau(a_2) & -i\tau\sigma(a_3) \\ a_1 & \sigma(a_0) & i\tau(a_3) & i\tau\sigma(a_2) \\ a_2 & -\sigma(a_3) & \tau(a_0) & -\tau\sigma(a_1) \\ a_3 & \sigma(a_2) & \tau(a_1) & \tau\sigma(a_0) \end{bmatrix} \right\}$$

where $a_0 = s_{01}\theta_1 + s_{02}\theta_2$, $a_1 = s_{03}\theta_1 + s_{04}\theta_2$, $a_2 = s_{11}\theta_1 + s_{12}\theta_2$, $a_3 = s_{13}\theta_1 + s_{14}\theta_2$ with $s_{kj} \in M\text{-QAM} \subset \mathbb{Z}[i]$, and $\{\theta_1, \theta_2 | \theta_i \in \mathcal{O}_{\mathbb{K}}\}$ is a suitable $\mathbb{Q}(i)$ -basis. From [7], we pick $\theta_1 = \alpha$, $\theta_2 = \alpha\theta$, where $\alpha = 1 + i(1 - \theta)$, $\theta = (1 + \sqrt{5})/2$, and $\{\alpha, \alpha\theta\}$ is now a basis of a principal ideal of $\mathcal{O}_{\mathbb{K}}$ generated by α . We now wish to prove that the STBC-scheme that is based on $\mathcal{S}_{4 \times 2}$ has the NVD property. To do so, it is sufficient from Theorem 2 to prove that $A\Upsilon(A) \neq i, \forall A \in \mathcal{A}$.

Proposition 3: Let $\mathcal{A} = (\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(\sqrt{5}), \sigma, -1)$. Then, $A\Upsilon(A) \neq i, \forall A \in \mathcal{A}$.

Proof: Let $A = a + \mathbf{j}b$, $a, b \in \mathbb{Q}(i, \sqrt{5})$. Suppose that

$$A\Upsilon(A) = i. \quad (32)$$

Now, if $b = 0$, then $a\tau(a) = i$ which is not a possibility in the Golden algebra (which has i as its non-norm element). If

$a = 0$, we have $\mathbf{j}b\mathbf{j}\tau(b) = i$ so that

$$\sigma(b)\tau(b) = -i. \quad (33)$$

Applying σ throughout in (33), we get $b\sigma\tau(b) = i$. Next, applying τ throughout in (33), we get $b\sigma\tau(b) = -i$ which leads to a contradiction. So, (33) is not true (Note that τ^2 is identity and $\tau\sigma = \sigma\tau$) and we can assume that $a, b \neq 0$. Now, applying Υ throughout in (32), we obtain $\Upsilon(A)A = i$. Hence,

$$(a + \mathbf{j}b)(\tau(a) + \mathbf{j}\tau(b)) = (\tau(a) + \mathbf{j}\tau(b))(a + \mathbf{j}b)$$

which leads to

$$\frac{\sigma(b)}{\sigma\tau(b)} = \sigma\left(\frac{b}{\tau(b)}\right) = \frac{b}{\tau(b)} \quad (34)$$

Hence, $b/\tau(b)$ is invariant under σ and hence belongs to $\mathbb{Q}(\sqrt{5})$. Also, from (32), we have

$$\begin{aligned} a\tau(a) - \sigma(b)\tau(b) &= i \\ b\tau(a) + \sigma(a)\tau(b) &= 0 \end{aligned} \quad (35)$$

so that

$$\frac{b}{\tau(b)} = -\frac{\sigma(a)}{\tau(a)}. \quad (36)$$

Using (36) in (35), we obtain

$$\frac{\tau(a)}{\sigma(a)}(a\sigma(a) + b\sigma(b)) = i.$$

Now, $a\sigma(a) + b\sigma(b)$ is invariant under σ and hence is in $\mathbb{Q}(\sqrt{5})$. So, $\tau(a)/\sigma(a)$ is imaginary and belongs to $\mathbb{Q}(i, \sqrt{5})$, using which in (36), we note that $b/\tau(b)$ is also imaginary. This contradicts the earlier result obtained below (34). Therefore, our assumption that $A\Upsilon(A) = i$ is false which proves the lemma. ■

Therefore, $\mathcal{S}_{4 \times 2}$ is a rate-2 STBC with full-diversity and equipped with the property of non-vanishing determinant.

1) *Minimum determinant:* When s_{ki} , $k = 0, 1$, $i = 1, \dots, 4$, take values from $\mathbb{Z}[i]$, from Corollary 1 the determinant of each of the codewords of $\mathcal{S}_{4 \times 2}$ belongs to $\mathbb{Z}[i]$. So, the minimum determinant of the unnormalized code is at least 1. However, noting that the entries of the i^{th} column of a codeword matrix, $i = 1, \dots, 4$, are all respectively multiples of α , $\sigma(\alpha)$, $\tau(\alpha)$, and $\sigma\tau(\alpha)$, the minimum determinant⁴ is a multiple of $|\alpha\sigma(\alpha)\tau(\alpha)\sigma\tau(\alpha)|^2 = |N_{\mathbb{K}/\mathbb{F}}(\alpha)|^4 = 25$ (σ is simply complex conjugation). When s_{ki} take values from an M -QAM with average energy E units, a normalization factor (see Note 1 in Section II) of $\frac{1}{\sqrt{4E|\alpha|^2(1+\theta^2)}} = \frac{1}{\sqrt{20E}}$ has to be taken into account. Further, since the difference between any two signal points in a QAM constellation is a

³While the constructed STBCs can be used for arbitrary number of receive antennas, they are full-rate only for MIDO systems.

⁴The entries of the Golden code are not just from $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[i, \theta]$ but from a principal ideal in $\mathcal{O}_{\mathbb{K}}$ generated by α . For details on this theory, one can refer to [7]

multiple of 2, the normalized minimum determinant of $\mathcal{S}_{4 \times 2}$ is $\delta_{\min}(\mathcal{S}_{4 \times 2}) = 25 \left(\frac{2}{\sqrt{20E}} \right)^8 = \frac{1}{25E^4}$.

2) *Relation with Srinath-Rajan code:* A codeword matrix of the SR-code is given by

$$\mathbf{S} = \begin{bmatrix} \mathbf{A} & e^{\frac{i\pi}{4}} \mathbf{C} \\ e^{\frac{i\pi}{4}} \mathbf{B} & \mathbf{D} \end{bmatrix}$$

where

$$\begin{aligned} \mathbf{A} &= \begin{bmatrix} x_{1I} + ix_{3Q} & -x_{2I} + ix_{4Q} \\ x_{2I} + ix_{4Q} & x_{1I} - ix_{3Q} \end{bmatrix}, \\ \mathbf{B} &= \begin{bmatrix} x_{5I} + ix_{7Q} & -x_{6I} + ix_{8Q} \\ x_{6I} + ix_{8Q} & x_{5I} - ix_{7Q} \end{bmatrix}, \\ \mathbf{C} &= \begin{bmatrix} x_{7I} + ix_{5Q} & -x_{8I} + ix_{6Q} \\ x_{8I} + ix_{6Q} & x_{7I} - ix_{5Q} \end{bmatrix}, \\ \mathbf{D} &= \begin{bmatrix} x_{3I} + ix_{1Q} & -x_{4I} + ix_{2Q} \\ x_{4I} + ix_{2Q} & x_{3I} - ix_{1Q} \end{bmatrix}, \end{aligned}$$

with x_{iI} and x_{iQ} being the real and imaginary parts respectively of the complex symbol x_i , $i = 1, \dots, 8$, and $x_i = e^{\frac{i \tan^{-1}(2)}{2}} s_i$, $s_i \in \mathbb{Z}[i]$ (i.e., from a suitable QAM constellation). Denoting $\tan^{-1}(2)/2$ by θ_g , we have

$$\begin{aligned} x_i &= \cos \theta_g s_{iI} - \sin \theta_g s_{iQ} + i(\sin \theta_g s_{iI} + \cos \theta_g s_{iQ}) \\ &= \sin \theta_g [\cot \theta_g s_{iI} - s_{iQ} + i(s_{iI} + \cot \theta_g s_{iQ})] \\ &= \sin \theta_g [\theta s_{iI} - s_{iQ} + i(s_{iI} + \theta s_{iQ})] \end{aligned}$$

where $\theta = (1 + \sqrt{5})/2$. So, it is easy to work out that $\mathbf{S} = \mathbf{U}' \mathbf{U}^H \mathbf{D}$, with $\mathbf{U} = \text{diag}[1, 1, e^{\frac{i\pi}{4}}, e^{\frac{i\pi}{4}}]$,

$$\mathbf{S}' = \begin{bmatrix} f_0 & -\sigma(f_1) & i\tau(f_2) & -i\sigma\tau(f_3) \\ f_1 & \sigma(f_0) & i\tau(f_3) & i\sigma\tau(f_2) \\ f_2 & -\sigma(f_3) & \tau(f_0) & -\sigma\tau(f_1) \\ f_3 & \sigma(f_2) & \tau(f_1) & \sigma\tau(f_0) \end{bmatrix} \quad (37)$$

where $f_0 = -s_{1Q} + is_{3I} + \theta(s_{1I} + is_{3Q})$, $f_1 = -s_{2Q} + is_{4I} + \theta(s_{2I} + is_{4Q})$, $f_2 = -s_{5Q} + is_{7I} + \theta(s_{5I} + is_{7Q})$, $f_3 = -s_{6Q} + is_{8I} + \theta(s_{6I} + is_{8Q})$, and $\mathbf{D} = \text{diag}[\sin \theta_g, \sin \theta_g, \theta \sin \theta_g, \theta \sin \theta_g]$. So, $f_i \in \mathbb{Z}[i, \theta]$ and it is easy to observe that a codeword matrix \mathbf{S} of $\mathcal{S}_{4 \times 2}$ constructed in this subsection has the structure $\mathbf{S} = \mathbf{S}' \mathbf{D}_1$ where \mathbf{S}' has the same algebraic structure as \mathbf{S}' in (37) and $\mathbf{D} = \text{diag}[\frac{\alpha}{\sqrt{5}}, \frac{\sigma(\alpha)}{\sqrt{5}}, \frac{\tau(\alpha)}{\sqrt{5}}, \frac{\sigma\tau(\alpha)}{\sqrt{5}}]$ (the scaling factor of $1/\sqrt{5}$ is for energy equalization). Clearly, the SR-code and $\mathcal{S}_{4 \times 2}$ have the same underlying algebraic structure and hence the same minimum determinant (this follows from the fact that $|\det(\mathbf{D})| = |\det(\mathbf{D}_1)| = 1/5$) and ML-decoding complexity. This also establishes that the STBC-scheme that is based on the SR-code has the NVD property, which had been previously only conjectured.

C. 6×2 MIDO system

We choose $\mathcal{A}_1 = (\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\omega), \tau, \omega)$, with $\theta = \zeta_7 + \zeta_7^{-1} = 2 \cos(\frac{2\pi}{7})$ and ζ_7 denoting the primitive 7th root of unity. \mathcal{A}_1 is the cyclic division algebra used to construct the perfect code for 3 transmit antennas [7]. τ is the generator of

$\text{Gal}(\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\omega))$ given by $\tau : \zeta_7 + \zeta_7^{-1} \mapsto \zeta_7^2 + \zeta_7^{-2}$. \mathcal{A} is chosen to be $(\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\theta), \sigma, -1)$. Since $\omega = (-1 + \sqrt{3}i)/2$, $\sigma(\omega) = \omega^2$. It is to be noted that $\gamma_M = \omega \notin \mathbb{Q}(\theta)$. The rate-2 STBC (unnormalized with respect to SNR) for 6 transmit antennas is given by

$$\mathcal{S}_{6 \times 2} = \left\{ \begin{bmatrix} \mathbf{A}_0 & \mathbf{O} & \omega \Upsilon^2(\mathbf{A}_1) \\ \mathbf{A}_1 & \Upsilon(\mathbf{A}_0) & \mathbf{O} \\ \mathbf{O} & \Upsilon(\mathbf{A}_1) & \Upsilon^2(\mathbf{A}_0) \end{bmatrix} \right\}$$

where

$$\mathbf{A}_k = \begin{bmatrix} \sum_{i=1}^3 s_{ki} \theta_i & -\sigma \left(\sum_{i=1}^3 s_{k(i+3)} \theta_i \right) \\ \sum_{i=1}^3 s_{k(i+3)} \theta_i & \sigma \left(\sum_{i=1}^3 s_{ki} \theta_i \right) \end{bmatrix}$$

with $s_{kj} \in M\text{-HEX} \subset \mathbb{Z}[\omega]$, $k = 0, 1$, $i = 1, \dots, 6$ and $\{\theta_1, \theta_2, \theta_3\}$, given by [7] $\theta_1 = 1 + \omega + \theta$, $\theta_2 = -1 - 2\omega + \omega\theta^2$, $\theta_3 = (-1 - 2\omega) + (1 + \omega)\theta + (1 + \omega)\theta^2$, is a basis of a principal ideal in $\mathcal{O}_{\mathbb{K}}$ generated by θ_1 . To prove that the STBC-scheme which is based on $\mathcal{S}_{6 \times 2}$ has the NVD property, it is sufficient to prove that $A\Upsilon(A)\Upsilon^2(A) \neq \omega$, $\forall A \in \mathcal{A}$. The proof is on similar lines to that of Proposition 3 and given in Appendix A.

1) *Minimum determinant:* When s_{ki} , $k = 0, 1$, $i = 1, \dots, 6$, take values from $\mathbb{Z}[\omega]$, from Corollary 1 the determinant of each of the codewords of $\mathcal{S}_{6 \times 2}$ belongs to $\mathbb{Z}[\omega]$. So, the minimum determinant of the unnormalized code is at least 1. However, the perfect code for 3 antennas has its entries from a principal ideal in $\mathcal{O}_{\mathbb{K}}$ generated by θ_1 . So, the minimum determinant is $|N_{\mathbb{K}/\mathbb{F}}(\theta_1)|^4 = 7^2 = 49$. When the constellation used is $M\text{-HEX}$ (so that the difference between any two signal points is a multiple of 2), after taking into account a normalization factor of $1/\sqrt{4E(|\theta_1|^2 + |\theta_2|^2 + |\theta_3|^2)} = 1/\sqrt{28E}$, the normalized minimum determinant of $\mathcal{S}_{6 \times 2}$ is $(49) \left(\frac{2}{\sqrt{28E}} \right)^{12} = \frac{1}{7^4 E^6}$.

D. 8×2 MIDO system

We choose \mathcal{A}_1 to be the cyclic division algebra used to construct the perfect code for 4 transmit antennas, i.e., $\mathcal{A}_1 = (\mathbb{Q}(i, \theta)/\mathbb{Q}(i), \tau, i)$ with $\theta = \zeta_{15} + \zeta_{15}^{-1} = 2 \cos(\frac{2\pi}{15})$ where ζ_{15} denotes the primitive 15th root of unity. Specifically, $\mathcal{A}_1 = \{a_0 + \mathbf{i}a_1 + \mathbf{i}^2 a_2 + a_3 \mathbf{i}^3, a_i \in \mathbb{Q}(i, \theta)\}$ with $\mathbf{i}^4 = i$, $\mathbf{i}a = \mathbf{i}\tau(a)$, $\forall a \in \mathbb{Q}(i, \theta)$ and τ is the generator of $\text{Gal}(\mathbb{Q}(i, \theta)/\mathbb{Q}(i))$ given by $\tau : \zeta_{15} + \zeta_{15}^{-1} \mapsto \zeta_{15}^2 + \zeta_{15}^{-2}$. \mathcal{A} is chosen to be $(\mathbb{Q}(i, \theta)/\mathbb{Q}(\theta), \sigma, -1)$. It is to be noted that $\gamma_M = i \notin \mathbb{Q}(\theta)$. The rate-2 STBC (unnormalized with respect to SNR) for 8 transmit antennas is given by

$$\mathcal{S}_{8 \times 2} = \left\{ \begin{bmatrix} \mathbf{A}_0 & \mathbf{O} & \mathbf{O} & i\Upsilon^3(\mathbf{A}_1) \\ \mathbf{A}_1 & \Upsilon(\mathbf{A}_0) & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \Upsilon(\mathbf{A}_1) & \Upsilon^2(\mathbf{A}_0) & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \Upsilon^2(\mathbf{A}_1) & \Upsilon^3(\mathbf{A}_0) \end{bmatrix} \right\}$$

where

$$\mathbf{A}_k = \begin{bmatrix} \sum_{i=1}^4 s_{ki} \theta_i & -\sigma \left(\sum_{i=1}^4 s_{k(i+4)} \theta_i \right) \\ \sum_{i=1}^4 s_{k(i+4)} \theta_i & \sigma \left(\sum_{i=1}^4 s_{ki} \theta_i \right) \end{bmatrix}$$

with $s_{kj} \in M\text{-QAM} \subset \mathbb{Z}[i]$, $k = 0, 1$, $j = 1, \dots, 8$ and $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ is a basis [7] of a principal ideal in $\mathcal{O}_{\mathbb{K}}$

$$\mathcal{S}_{12 \times 2} = \left\{ \begin{bmatrix} \mathbf{A}_0 & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & -\omega \Upsilon^5(\mathbf{A}_1) \\ \mathbf{A}_1 & \Upsilon(\mathbf{A}_0) & \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \Upsilon(\mathbf{A}_1) & \Upsilon^2(\mathbf{A}_0) & \mathbf{O} & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \Upsilon^2(\mathbf{A}_1) & \Upsilon^3(\mathbf{A}_0) & \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \Upsilon^3(\mathbf{A}_1) & \Upsilon^4(\mathbf{A}_0) & \mathbf{O} \\ \mathbf{O} & \mathbf{O} & \mathbf{O} & \mathbf{O} & \Upsilon^4(\mathbf{A}_1) & \Upsilon^5(\mathbf{A}_0) \end{bmatrix}, \mathbf{A}_k = \begin{bmatrix} z_{k0} & -\sigma(z_{k1}) \\ z_{k1} & \sigma(z_{k0}) \end{bmatrix} \right\}. \quad (38)$$

generated by θ_1 , where $\theta_1 = \alpha$, $\theta_2 = \alpha\theta$, $\theta_3 = \alpha\theta(-3 + \theta^2)$, $\theta_4 = \alpha(-1 - 3\theta + \theta^2 + \theta^3)$, with $\alpha = 1 - 3i + i\theta^2$. To prove that the STBC-scheme which is based on $\mathcal{S}_{8 \times 2}$ has the NVD property, it is sufficient to prove that $A\Upsilon(A)\Upsilon^2(A)\Upsilon^3(A) \neq i$, $\forall A \in \mathcal{A}$. This is done in Appendix B.

1) *Minimum determinant*: When s_{ki} , $k = 0, 1$, $i = 1, \dots, 8$, take values from $\mathbb{Z}[i]$, from Corollary 1 the determinant of each of the codewords of $\mathcal{S}_{8 \times 2}$ belongs to $\mathbb{Z}[i]$ and hence the minimum determinant of the unnormalized code is at least 1. However, the perfect code for 4 antennas has its entries from a principal ideal in $\mathcal{O}_{\mathbb{K}}$ generated by θ_1 whose norm has modulus $\sqrt{45}$. Hence, the minimum determinant is $|N_{\mathbb{K}/\mathbb{F}}(\theta_1)|^4 = 45^2$. When the constellation used is M -QAM, after taking into account a normalization factor of $1/\sqrt{4E \sum_{i=1}^4 |\theta_i|^2} = 1/\sqrt{60E}$, the normalized minimum determinant of $\mathcal{S}_{8 \times 2}$ is $(45^2) \left(\frac{2}{\sqrt{60E}}\right)^{16} = \frac{1}{25(15)^4 E^8}$.

E. 12×2 MIMO system

We choose \mathcal{A}_1 to be the cyclic division algebra used to construct the perfect code for 6 transmit antennas, i.e., $\mathcal{A}_1 = (\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\omega), \tau, -\omega)$ with $\theta = \zeta_{28} + \zeta_{28}^{-1} = 2\cos(\frac{\pi}{14})$ where ζ_{28} denotes the primitive 28^{th} root of unity. Specifically, $\mathcal{A}_1 = \{\sum_{k=0}^5 \mathbf{i}^k a_k, a_k \in \mathbb{Q}(\omega, \theta)\}$ with $\mathbf{i}^6 = -\omega$, $\mathbf{a}\mathbf{i} = \mathbf{i}\tau(a)$, $\forall a \in \mathbb{Q}(\omega, \theta)$ and τ is the generator of $\text{Gal}(\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\omega))$ given by $\tau : \zeta_{28} + \zeta_{28}^{-1} \mapsto \zeta_{28}^2 + \zeta_{28}^{-2}$. \mathcal{A} is chosen to be $(\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\theta), \sigma, -1)$. It is clear that $\gamma_M = -\omega \notin \mathbb{Q}(\theta)$. The rate-2 STBC (unnormalized with respect to SNR) for 12 transmit antennas is given by (38) at the top of the page with

$$\begin{bmatrix} z_{ki} \\ \tau(z_{ki}) \\ \tau^2(z_{ki}) \\ \tau^3(z_{ki}) \\ \tau^4(z_{ki}) \\ \tau^5(z_{ki}) \end{bmatrix} = \mathbf{R} \begin{bmatrix} s_{k(6i+1)} \\ s_{k(6i+2)} \\ s_{k(6i+3)} \\ s_{k(6i+4)} \\ s_{k(6i+5)} \\ s_{k(6i+6)} \end{bmatrix}, \quad k = 0, 1, \quad i = 0, 1,$$

where $s_{kj} \in M\text{-HEX} \subset \mathbb{Z}[\omega]$, $k = 0, 1$, $j = 1, \dots, 24$ and \mathbf{R} , defined by (7), is obtained from [7] and shown in (39) at the top of the next page.

As for the previous STBCs, to prove that the STBC-scheme that is based on $\mathcal{S}_{12 \times 2}$ has the NVD property, it is sufficient to show that $A\Upsilon(A)\Upsilon^2(A) \cdots \Upsilon^5(A) \neq -\omega$, $\forall A \in \mathcal{A}$ and this is done in Appendix C.

1) *Minimum determinant*: From Corollary 1, the minimum determinant of the unnormalized code is 1. Since the entries of the perfect code for 6 antennas are not in a principal ideal, a lower bound on the minimum determinant of the unnormalized code is 1. It can be checked that the norm of

each row of \mathbf{R} is $\sqrt{14}$. So, taking into account a normalization factor of $1/\sqrt{(4)(14)E} = \sqrt{56E}$, the normalized minimum determinant of $\mathcal{S}_{12 \times 2}$ whose symbols take values from M -HEX is at least $\left(\frac{1}{\sqrt{14E}}\right)^{24} = \left(\frac{1}{14E}\right)^{12}$.

V. ML-DECODING COMPLEXITY

In this section, we analyze the ML-decoding complexity of the constructed STBCs as a function of the constellation size M . When the constellation used is M -QAM (for 4 and 8 transmit antennas), we assume it to be a square QAM so that the real and imaginary parts are separable. Consider the ML-decoding metric given by $\|\mathbf{Y} - \rho\mathbf{H}\mathbf{S}\|^2$, which is to be minimized over all possible codewords $\mathbf{S} \in \mathcal{S}$. We have

$$\begin{aligned} \|\mathbf{Y} - \rho\mathbf{H}\mathbf{S}\|^2 &= \text{tr}[(\mathbf{Y} - \rho\mathbf{H}\mathbf{S})(\mathbf{Y} - \rho\mathbf{H}\mathbf{S})^H] \\ &= \text{tr}(\mathbf{Y}\mathbf{Y}^H - \rho\mathbf{Y}\mathbf{S}^H\mathbf{H}^H \\ &\quad - \rho\mathbf{H}\mathbf{S}\mathbf{Y}^H + \rho^2\mathbf{H}\mathbf{S}\mathbf{S}^H\mathbf{H}^H) \\ &= \text{tr}(\mathbf{Y}\mathbf{Y}^H) - \text{tr}(\rho\mathbf{Y}\mathbf{S}^H\mathbf{H}^H) \\ &\quad - \text{tr}(\rho\mathbf{H}\mathbf{S}\mathbf{Y}^H) + \text{tr}(\rho^2\mathbf{H}\mathbf{S}\mathbf{S}^H\mathbf{H}^H). \end{aligned}$$

The only term in the ML-decoding metric that has an entanglement of the information symbols is $\text{tr}(\rho^2\mathbf{H}\mathbf{S}\mathbf{S}^H\mathbf{H}^H)$. Hence, $\mathbf{S}\mathbf{S}^H$ defines the ML-decoding complexity of the STBC. Now, let $z_1 = \sum_{i=1}^n s_{1i}\theta_i$, $z_2 = \sum_{i=1}^n s_{2i}\theta_i$, where s_{ki} take values from either QAM or HEX constellations, $\theta_i \in \mathbb{C}$. If the transmitted codeword is

$$\mathbf{S} = \begin{bmatrix} z_1 & -\sigma(z_2) \\ z_2 & \sigma(z_1) \end{bmatrix}$$

where σ performs complex conjugation, $\mathbf{S}\mathbf{S}^H = (|z_1|^2 + |z_2|^2)\mathbf{I}$. Hence, the group of symbols $\{s_{1i}, i = 1, \dots, n\}$ that z_1 consists of are disentangled in the decoding metric from $\{s_{2i}, i = 1, \dots, n\}$ that z_2 consists of. So, $\{s_{1i}, i = 1, \dots, n\}$ can be decoded independently of $\{s_{2i}, i = 1, \dots, n\}$. In addition, if s_{ki} take values from a square QAM constellation and θ_i , $i = 1, \dots, n$, are of the form $\theta_i = \alpha\theta'_i$ where $\alpha \in \mathbb{C}$ and $\theta'_i \in \mathbb{R}$, then within each group $\{s_{ki}, i = 1, \dots, n\}$, $k = 1, 2$, the group comprising the real parts of each symbol is separable from the group comprising the imaginary parts. Hence,

- 1) when s_{ki} take values from a square QAM, the four groups - $\{s_{1iI}, i = 1, \dots, n\}$, $\{s_{1iQ}, i = 1, \dots, n\}$, $\{s_{2iI}, i = 1, \dots, n\}$ and $\{s_{2iQ}, i = 1, \dots, n\}$, are independently decodable of one another.
- 2) when s_{ki} take values from a HEX constellation, the two groups $\{s_{1i}, i = 1, \dots, n\}$ and $\{s_{2i}, i = 1, \dots, n\}$ are independently decodable of one another.

$$\mathbf{R} = \begin{bmatrix} 1.9498 & 1.3019 - 0.8660i & -0.0549 - 0.8660i & -1.7469 - 0.8660i & 1.5636 & 0.8677 \\ 0.8677 & -1.7469 - 0.8660i & 1.3019 - 0.8660i & -0.0549 - 0.8660i & -1.9498 & 1.5636 \\ 1.5636 & -0.0549 - 0.8660i & -1.7469 - 0.8660i & 1.3019 - 0.8660i & -0.8677 & -1.9498 \\ -1.9498 & 1.3019 - 0.8660i & -0.0549 - 0.8660i & -1.7469 - 0.8660i & -1.5636 & -0.8677 \\ -0.8677 & -1.7469 - 0.8660i & 1.3019 - 0.8660i & -0.0549 - 0.8660i & 1.9498 & -1.5636 \\ -1.5636 & -0.0549 - 0.8660i & -1.7469 - 0.8660i & 1.3019 - 0.8660i & 0.8677 & 1.9498 \end{bmatrix}. \quad (39)$$

So, we have the following proposition.

Proposition 4: Let the codeword matrices of an STBC \mathcal{S} be block diagonal of the form $\mathbf{S} = \text{diag}[\mathbf{A}, \Upsilon(\mathbf{A}), \dots, \Upsilon^{n-1}(\mathbf{A})]$, where

$$\mathbf{A} = \begin{bmatrix} \sum_{i=1}^n s_{1i}\theta_i & -\sigma(\sum_{i=1}^n s_{2i}\theta_i) \\ \sum_{i=1}^n s_{2i}\theta_i & \sigma(\sum_{i=1}^n s_{1i}\theta_i) \end{bmatrix},$$

$$\Upsilon^l(\mathbf{A}) = \begin{bmatrix} \tau^l(\sum_{i=1}^n s_{1i}\theta_i) & -\sigma\tau^l(\sum_{i=1}^n s_{2i}\theta_i) \\ \tau^l(\sum_{i=1}^n s_{2i}\theta_i) & \sigma\tau^l(\sum_{i=1}^n s_{1i}\theta_i) \end{bmatrix}$$

and $\{\theta_i, i = 1, \dots, n | \theta_i \in \mathcal{O}_{\mathbb{K}}\}$ is the $\mathbb{Q}(i)$ -basis (or $\mathbb{Q}(\omega)$ -basis) of a number field \mathbb{K} which is a Galois extension of degree n over $\mathbb{Q}(i)$ (respectively $\mathbb{Q}(\omega)$) with Galois group $\langle \tau \rangle$. If $\theta_i, i = 1, \dots, n$, are of the form $\theta_i = \alpha\theta'_i$ where $\alpha \in \mathbb{C}$ and $\theta'_i \in \mathbb{R}$, then \mathcal{S} is

- 1) four-group decodable if s_{ki} take values from QAM.
- 2) two-group decodable if s_{ki} take values from HEX.

Proof: The proof is trivial and follows from the argument preceding the proposition. ■

Following Proposition 4, the ML-decoding complexity of the codes constructed is easy to analyze. For the STBCs for 4×2 and 8×2 MIDO system, the first $2n$ complex symbols ($n = 2$ and 4 respectively for 4×2 and 8×2 MIDO systems) corresponding to \mathbf{A}_0 are conditionally four-group decodable for each of the possibilities for the remaining symbols (i.e., the $2n$ symbols that constitute \mathbf{A}_1). So, assuming the usage of M -QAM, the ML-decoding complexity of $\mathcal{S}_{4 \times 2}$ is of the order of $(M^4)(M)$ - the factor M^4 is due to the joint evaluation of the last 4 complex symbols and the factor M is due to independence in evaluation of each of the first 4 symbols once the last 4 are fixed. In addition, by employing hard-limiting [2] to evaluate the real part of each of the first 4 symbols, the complexity can be further reduced by a factor of \sqrt{M} (M is assumed to be a square). Hence, the ML-decoding complexity of $\mathcal{S}_{4 \times 2}$ is of the order of $M^{4.5}$. By a similar analysis, the ML-decoding complexity of $\mathcal{S}_{8 \times 2}$ is of the order of $(M^8)(M^{1.5}) = M^{9.5}$.

For $\mathcal{S}_{6 \times 2}$ and $\mathcal{S}_{12 \times 2}$, the first $2n$ complex symbols ($n = 3$ and 6 respectively for $\mathcal{S}_{6 \times 2}$ and $\mathcal{S}_{12 \times 2}$) corresponding to the diagonal block matrices are conditionally two-group decodable for each of the possibilities for the remaining $2n$ symbols. Hence, the ML-decoding complexity of $\mathcal{S}_{6 \times 2}$ is of the order of $(M^6)(M^{2.5}) = M^{8.5}$ and that of $\mathcal{S}_{12 \times 2}$ is of the order of $(M^{12})(M^{5.5}) = M^{17.5}$ (the reduction by a factor of \sqrt{M} is again due to the usage of hard-limiting). Table I captures the salient features of the constructed codes along with their comparison with known best STBCs.

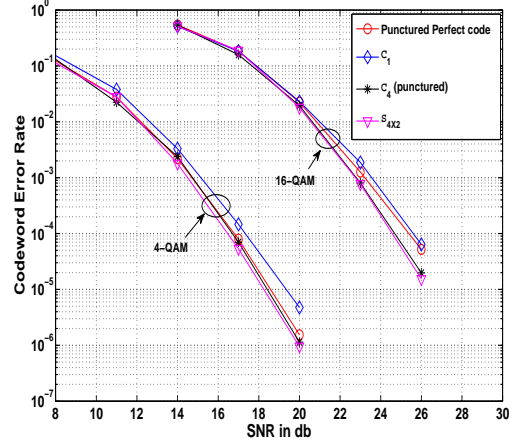


Fig. 1. CER performance of various rate-2 STBCs for the 4×2 system with 4-/16-QAM

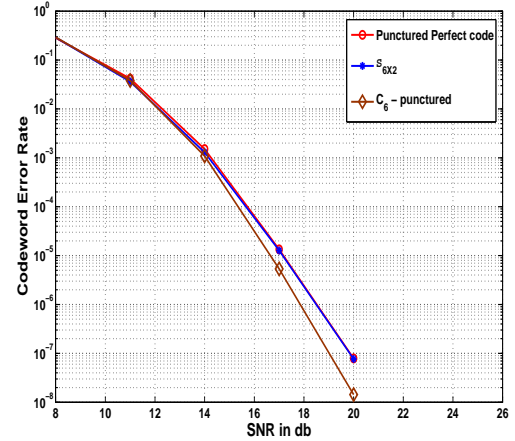


Fig. 2. CER performance of the punctured Perfect code for 6 Tx and $\mathcal{S}_{6 \times 2}$ for the 6×2 system with 4-QAM

VI. COMPARISON WITH EXISTING STBCS

We compare the performance of the STBCs constructed in this paper with the best known STBCs that have a provable NVD.

A. 4×2 MIDO system

As rival codes for $\mathcal{S}_{4 \times 2}$, we consider the following STBCs - the punctured perfect code for 4 transmit antennas (two of its layers have zero entries), the rate-2 STBC obtained in [17] (also in [1]), which we call \mathcal{C}_1 , and a new STBC obtained by puncturing \mathcal{C}_4 [28]. \mathcal{C}_1 is also obtained from the same

CDA that \mathcal{C}_4 is obtained from, but with a change of basis. Specifically, a codeword matrix of \mathcal{C}_1 has its entries belonging to $\mathbb{Q}(i, \sqrt{5})$ and the basis is the same as that for the Golden code, i.e., $\{\alpha, \alpha\theta\}$, with α and θ as defined in Subsection IV-B. Further, σ sends $\sqrt{5}$ to $-\sqrt{5}$ and σ^2 fixes $\mathbb{Q}(i, \sqrt{5})$. \mathcal{C}_1 has the same coding gain as $\mathcal{S}_{4 \times 2}$ but not its ML-decoding complexity. The third rival code is obtained from \mathcal{C}_4 by simply puncturing the symbols corresponding to the basis elements ζ_5^2 and ζ_5^3 , i.e., the entries of the first column of the codeword matrices are of the form $s_{i1} + s_{i2}\zeta_5$. This STBC has the best coding gain which can be explicitly calculated and is shown in Table I. We haven't considered the BHV code [15] as it is not a full-diversity STBC. We also have not considered the other full-diversity STBCs proposed in [16] - [20] since these codes have not been constructed with a focus on coding gain but only with an intention of having fast-decodability with a provable NVD. The constellations used in our simulations are 4-QAM and 16-QAM.

Fig 1 reveals that surprisingly, $\mathcal{S}_{4 \times 2}$ has the best error performance among all codes under comparison although the punctured \mathcal{C}_4 has the best coding gain. This can possibly be attributed to the multiplicity of the minimum determinant - the number of codeword-difference matrix pairs whose squared absolute value of determinant is the minimum determinant. We believe that the punctured \mathcal{C}_4 has more such pairs since it is obtained by puncturing \mathcal{C}_4 and our method of puncturing might not be efficient. Punctured \mathcal{C}_4 loses only slightly to $\mathcal{S}_{4 \times 2}$ and these two codes clearly beat the punctured perfect code and \mathcal{C}_1 for both 4- and 16-QAM. Also surprising is the fact that \mathcal{C}_1 has the poorest performance although it has the same normalized minimum determinant as $\mathcal{S}_{4 \times 2}$ which may again be attributed to the multiplicity of the minimum determinant.

B. 6×2 MIDO system

For this system, the rival codes for $\mathcal{S}_{6 \times 2}$ are the punctured perfect code for 6 antennas [7] (4 layers punctured) and punctured \mathcal{C}_6 [28]. \mathcal{C}_6 is obtained from the CDA $(\mathbb{Q}(\omega, \zeta_7)/\mathbb{Q}(\omega), \tau : \zeta_7 \mapsto \zeta_7^3, -\omega)$, where ζ_7 is the primitive 7th root of unity. The entries of the first column of the codeword matrices of punctured \mathcal{C}_6 are of the form $s_{i1} + s_{i2}\zeta_7$, $s_{ij} \in M$ -HEX. The fast-decodable STBC (VHO-code) for the 6×2 MIDO system in [1] has the least ML-decoding complexity (see Table I) but has not been optimized for performance. Moreover, its non-norm element is $-3/4$ whose modulus is not unity. This implies that the VHO-code is not well shaped and so, we have not considered it in our simulations. All the STBCs use 4-HEX constellation. Fig 2 shows that $\mathcal{S}_{6 \times 2}$ and punctured perfect code have a very similar error performance which is natural since both have nearly the same normalized minimum determinants (for the punctured perfect code, only the upper bound and the lower bound exist, but it is likely that the upper bound is the actual normalized minimum determinant). The best performance is that of punctured \mathcal{C}_6 which has the largest normalized minimum determinant. However, $\mathcal{S}_{6 \times 2}$ has the least ML-decoding complexity among the three codes.

VII. DISCUSSION

In this paper, we proposed a new method to obtain full-diversity, rate-2 STBCs which, unlike existing full-diversity STBCs, are not obtainable as matrix representations of division algebras. We then constructed rate-2, fast-decodable STBCs for 4×2 , 6×2 , 8×2 and 12×2 systems which have large normalized minimum determinants and STBC-schemes consisting of these STBCs have a non-vanishing determinant (NVD) so that they are DMT-optimal for their respective MIDO systems. We also showed that the Srinath-Rajan code has the same algebraic structure as the STBC constructed in this paper for the 4×2 system, thereby proving a previous conjecture that the STBC-scheme based on the Srinath-Rajan code has the NVD property and hence is DMT-optimal for the 4×2 system. However, there is still scope for improvement. Firstly, with the exception of the STBC for 4×2 MIDO system, the remaining STBCs in this paper have a lot of zero entries and naturally, there is the issue of high peak to average power ratio (PAPR) which needs to be lowered. Secondly, it is natural to seek conditions that enable the construction of higher rate codes (rate > 2) with high coding gain and fast-decodability on the lines of the STBCs constructed in this paper. These are the possible directions for future research.

APPENDIX A

PROOF THAT $A\Upsilon(A)\Upsilon^2(A) \neq \omega$, $\forall A \in (\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\theta), \sigma, -1)$.

Let $A = a + \mathbf{j}b$, $a, b \in \mathbb{Q}(\omega, \theta)$ such that

$$A\Upsilon(A)\Upsilon^2(A) = \omega. \quad (40)$$

Firstly, $a \neq 0$ since otherwise $(\mathbf{j}b)(\mathbf{j}\tau(b))(\mathbf{j}\tau^2(b)) = \omega$ which is not possible. Secondly, $b \neq 0$ since $a\tau(a)\tau^2(a) \neq \omega$ for any $a \in \mathbb{Q}(\omega, \theta)$ (for ω is a non-norm element in \mathcal{A}_1). Hence, we assume that $a, b \neq 0$. Applying Υ^2 throughout (40), we obtain $\Upsilon^2(A)A\Upsilon(A) = \omega$ so that $A\Upsilon(A)\Upsilon^2(A) = \Upsilon^2(A)A\Upsilon(A)$. Now, $A\Upsilon(A) = x + \mathbf{j}\sigma(y)$ where $x = a\tau(a) - \sigma(b)\tau(b)$, $\sigma(y) = b\tau(a) + \sigma(a)\tau(b)$. So,

$$(x + \mathbf{j}\sigma(y))(\tau^2(a) + \mathbf{j}\tau^2(b)) = (\tau^2(a) + \mathbf{j}\tau^2(b))(x + \mathbf{j}\sigma(y))$$

from which we have

$$\sigma(y)\tau^2(a) + \sigma(x)\tau^2(b) = \sigma\tau^2(a)\sigma(y) + x\tau^2(b). \quad (41)$$

From (40), we obtain

$$x\tau^2(a) - y\tau^2(b) = \omega \quad (42)$$

$$\sigma(x)\tau^2(b) + \sigma(y)\tau^2(a) = 0. \quad (43)$$

If $x = 0$, then $y = 0$ (since $a \neq 0$) and (42) is not true. So, we can assume $x \neq 0$. Using (41) and (43), we get

$$\frac{\sigma(y)}{\tau^2(b)} = -\frac{x}{\sigma\tau^2(a)} = -\frac{\sigma(x)}{\tau^2(a)}$$

so that $\frac{x}{\sigma\tau^2(a)} = \sigma\left(\frac{x}{\sigma\tau^2(a)}\right)$. Therefore, $x/\sigma\tau^2(a)$ is real-valued and belongs to $\mathbb{Q}(\theta)$. Now, using (43) in (42), we get

$$\frac{\tau^2(a)}{\sigma(x)}[x\sigma(x) + y\sigma(y)] = \omega$$

Since $x\sigma(x) + y\sigma(y)$ is invariant under σ and hence real-valued, $\frac{\tau^2(a)}{\sigma(x)}$ must be complex-valued which contradicts the previous result. Hence, (40) is false and there exists no $A \in \mathcal{A}$ such that $A\Upsilon(A)\Upsilon^2(A) = \omega$.

APPENDIX B

PROOF THAT $A\Upsilon(A)\Upsilon^2(A)\Upsilon^3(A) \neq i, \forall A \in (\mathbb{Q}(i, \theta)/\mathbb{Q}(\theta), \sigma, -1)$.

Let $A = a + \mathbf{j}b, a, b \in \mathbb{Q}(i, \theta)$ such that

$$A\Upsilon(A)\Upsilon^2(A)\Upsilon^3(A) = i. \quad (44)$$

Applying Υ^2 throughout (44), we obtain $\Upsilon^2(A)\Upsilon^3(A)A\Upsilon(A) = i$ so that $A\Upsilon(A)\Upsilon^2(A)\Upsilon^3(A) = \Upsilon^2(A)\Upsilon^3(A)A\Upsilon(A)$. Let $A\Upsilon(A) = x + \mathbf{j}y$ where $x = a\tau(a) - \sigma(b)\tau(b), y = b\tau(a) + \sigma(a)\tau(b)$. So, we have

$$(x + \mathbf{j}y)(\tau^2(x) + \mathbf{j}\tau^2(y)) = (\tau^2(x) + \mathbf{j}\tau^2(y))(x + \mathbf{j}y)$$

from which we obtain

$$y\tau^2(x) + \sigma(x)\tau^2(y) = \sigma\tau^2(x)y + x\tau^2(y). \quad (45)$$

From (44), we obtain

$$x\tau^2(x) - \sigma(y)\tau^2(y) = i \quad (46)$$

$$\sigma(x)\tau^2(y) + y\tau^2(x) = 0. \quad (47)$$

Now, if $x = 0$,

$$\sigma(y)\tau^2(y) = -i. \quad (48)$$

By applying σ and τ^2 separately throughout (48), we obtain $y\sigma\tau^2(y) = i$ and $y\sigma\tau^2(y) = -i$ which contradict each other. Hence, $x \neq 0$. On the other hand, if $y = 0$, then $x\tau^2(x) = i$ and applying τ we get $\tau(x)\tau^3(x) = i$ so that $x\tau^2(x)\tau(x)\tau^3(x) = (i)(i) = -1$. Since $x \in \mathbb{Q}(i, \theta)$, this implies that there exists some $x \in \mathbb{Q}(i, \theta)$ such that $N_{\mathbb{Q}(i, \theta)/\mathbb{Q}(i)}(x) = -1$. This is not true since i^t is not a norm of any field element of $\mathbb{Q}(i, \theta)$ for $t = 1, 2, 3$. Hence, we can assume that $x, y \neq 0$. Using (45) and (47), we get

$$-\frac{\sigma\tau^2(x)}{x} = \frac{\tau^2(y)}{y} = -\frac{\tau^2(x)}{\sigma(x)}$$

so that $\frac{\tau^2(x)}{\sigma(x)} = \sigma\left(\frac{\tau^2(x)}{\sigma(x)}\right)$. Therefore, $\frac{\tau^2(x)}{\sigma(x)}$ is real-valued and belongs to $\mathbb{Q}(\theta)$. Now, using (47) in (46), we get

$$\frac{\tau^2(x)}{\sigma(x)}[x\sigma(x) + y\sigma(y)] = i$$

Since $x\sigma(x) + y\sigma(y)$ is invariant under σ and hence real-valued. So, it must be that $\frac{\tau^2(x)}{\sigma(x)}$ is complex-valued which contradicts the previous result. Hence, (44) is false and there exists no $A \in \mathcal{A}$ such that $A\Upsilon(A)\Upsilon^2(A)\Upsilon^3(A) = i$.

APPENDIX C

PROOF THAT $A\Upsilon(A)\Upsilon^2(A) \cdots \Upsilon^5(A) \neq -\omega, \forall A \in (\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\theta), \sigma, -1)$.

Let $A = a + \mathbf{j}b, a, b \in \mathbb{Q}(\omega, \theta)$ such that

$$A\Upsilon(A)\Upsilon^2(A) \cdots \Upsilon^5(A) = -\omega. \quad (49)$$

Applying Υ^3 throughout (49), we observe that $A\Upsilon(A)\Upsilon^2(A)$ and $\Upsilon^3(A)\Upsilon^4(A)\Upsilon^5(A)$ commute. Let $A\Upsilon(A)\Upsilon^2(A) = x + \mathbf{j}y$ where $x = x'\tau^2(a) - \sigma(y')\tau^2(b), y = y'\tau^2(a) + \sigma(x')\tau^2(b)$ with $x' = a\tau(a) - \sigma(b)\tau(b), y' = b\tau(a) + \sigma(a)\tau(b)$. So, we have

$$(x + \mathbf{j}y)(\tau^3(x) + \mathbf{j}\tau^3(y)) = (\tau^3(x) + \mathbf{j}\tau^3(y))(x + \mathbf{j}y)$$

from which we obtain

$$y\tau^3(x) + \sigma(x)\tau^3(y) = \sigma\tau^3(x)y + x\tau^3(y). \quad (50)$$

From (49), we obtain

$$x\tau^3(x) - \sigma(y)\tau^3(y) = -\omega \quad (51)$$

$$\sigma(x)\tau^3(y) + y\tau^3(x) = 0. \quad (52)$$

Now, if $x = 0$,

$$\sigma(y)\tau^3(y) = \omega. \quad (53)$$

By applying σ and τ^3 separately throughout (53), we obtain $y\sigma\tau^3(y) = \omega^2$ (for $\sigma(\omega) = \omega^2$) and $y\sigma\tau^3(y) = \omega$, which contradict each other. Hence, $x \neq 0$. On the other hand, if $y = 0$, then $x\tau^3(x) = -\omega$ and therefore, $\tau(x)\tau^4(x) = -\omega, \tau^2(x)\tau^5(x) = -\omega$. Using these results, we arrive at

$$(x\tau^3(x))(\tau(x)\tau^4(x))(\tau^2(x)\tau^5(x)) = (-\omega)^3 = -1. \quad (54)$$

Since $x \in \mathbb{Q}(\omega, \theta)$, (54) implies that there exists some $x \in \mathbb{Q}(\omega, \theta)$ such that $N_{\mathbb{Q}(\omega, \theta)/\mathbb{Q}(\omega)}(x) = -1$. This is not true since $(-\omega)^t$ is not a norm of any field element of $\mathbb{Q}(\omega, \theta)$ for $t = 1, \dots, 5$. Hence, we can assume that $x, y \neq 0$. Using (45) and (47), we get

$$-\frac{\sigma\tau^3(x)}{x} = \frac{\tau^3(y)}{y} = -\frac{\tau^3(x)}{\sigma(x)}$$

so that $\frac{\tau^3(x)}{\sigma(x)} = \sigma\left(\frac{\tau^3(x)}{\sigma(x)}\right)$. Therefore, $\frac{\tau^3(x)}{\sigma(x)}$ is real-valued and belongs to $\mathbb{Q}(\theta)$. Now, using (52) in (51), we get

$$\frac{\tau^3(x)}{\sigma(x)}[x\sigma(x) + y\sigma(y)] = \omega$$

Since $x\sigma(x) + y\sigma(y)$ is invariant under σ and hence real-valued, $\frac{\tau^3(x)}{\sigma(x)}$ has to be complex-valued which contradicts the previous result. Hence, (49) is false and there exists no $A \in \mathcal{A}$ such that $A\Upsilon(A)\Upsilon^2(A) \cdots \Upsilon^5(A) = -\omega$.

ACKNOWLEDGEMENTS

We thank Dr. Nadya Markin for useful discussions on the topic.

REFERENCES

- [1] R. Vehkalahti, C. Hollanti, and F. Oggier, "Fast-Decodable Asymmetric Space-Time Codes from Division Algebras," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2362-2385, Apr. 2012.
- [2] K. P. Srinath and B. S. Rajan, "Low ML-Decoding Complexity, Large Coding Gain, Full-Rate, Full-Diversity STBCs for 2×2 and 4×2 MIMO Systems," *IEEE J. Sel. Topics Signal Process.*, vol. 3, no. 6, pp. 916-927, Dec. 2009.

- [3] V. Tarokh, N. Seshadri, and A. R. Calderbank, "Space time codes for high data rate wireless communication : performance criterion and code construction," *IEEE Trans. Inf. Theory*, vol. 44, no. 2, pp. 744 - 765, Mar. 1998.
- [4] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 8, pp. 1451-1458, Oct. 1998.
- [5] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, High-rate Space-Time Block Codes from Division Algebras," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2596-2616, Oct. 2003.
- [6] J. C. Belfiore, G. Rekaya, and E. Viterbo, "The Golden Code: A 2×2 full rate space-time code with non-vanishing determinants," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1432-1436, Apr. 2005.
- [7] F. Oggier, G. Rekaya, J. C. Belfiore, and E. Viterbo, "Perfect space time block codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3885-3902, Sep. 2006.
- [8] P. Elia, K. R. Kumar, S. A. Pawar, P. V. Kumar, and H.-F. Lu, "Explicit Space-Time Codes Achieving the Diversity-Multiplexing Gain Tradeoff," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3869-3884, Sep. 2006.
- [9] P. Elia, B. A. Sethuraman, and P. V. Kumar, "Perfect Space-Time Codes for Any Number of Antennas," *IEEE Trans. Inf. Theory*, vol. 53, no. 11, pp. 3853-3868, Nov. 2007.
- [10] Z. A. Khan and B. S. Rajan, "Single-Symbol Maximum-Likelihood Decodable Linear STBCs," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2062-2091, May 2006.
- [11] D. N. Dao, C. Yuen, C. Tellambura, Y. L. Guan, and T. T. Tjhung, "Four-group decodable space-time block codes," *IEEE Trans. Signal Process.*, vol. 56, no. 1, pp. 424-430, Jan. 2008.
- [12] S. Karmakar and B. S. Rajan, "Multigroup-Decodable STBCs from Clifford Algebras," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 223-231, Jan. 2009.
- [13] G. S. Rajan and B. S. Rajan, "Multi-group ML Decodable Collocated and Distributed Space Time Block Codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3221-3247, Jul. 2010.
- [14] The Global Standard for Digital Television DVB Project [Online]. Available: <http://www.dvb.org>.
- [15] E. Biglieri, Y. Hong, and E. Viterbo, "On fast-decodable space-time block codes," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 524-530, Feb. 2009.
- [16] F. Oggier, R. Vehkalahti, and C. Hollanti, "Fast-decodable MIMO codes from crossed product algebras," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Austin, TX, June 2010.
- [17] F. Oggier, C. Hollanti, and R. Vehkalahti, "An algebraic MIMO-MISO code construction," in *Proc. Int. Conf. Signal Process. and Commun. (SPCOM 2010)*, Bangalore, India, July 2010.
- [18] R. Vehkalahti, C. Hollanti, and J. Lahtonen, "A family of cyclic division algebra based fast-decodable 4×2 space-time block codes," in *Proc. Int. Symp. Inf. Theory and Appl. (ISITA)*, Taichung, Taiwan, Oct. 2010.
- [19] L. Luzzi and F. Oggier, "A family of fast-decodable MIMO codes from crossed-product algebras over \mathbb{Q} ," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, St. Petersburg, Russia, July - Aug. 2011.
- [20] N. Markin and F. Oggier, "Iterated Space-Time Code Constructions from Cyclic Algebras," available online at arXiv, arXiv:1205.5134v1 [cs.IT].
- [21] S. Pumpluen and T. Unger, "Space-time block codes from nonassociative division algebras," *Adv. Math. Commun.* 5, no. 3, 449-471, 2011.
- [22] K. P. Srinath and B. S. Rajan, "DMT-optimal, Low ML-Complexity STBC-Schemes for Asymmetric MIMO Systems", available online at arXiv, arXiv:1201.1997v2 [cs.IT].
- [23] L. Zheng and D. Tse, "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1073-1096, May 2003.
- [24] B. Hassibi and B. Hochwald, "High-rate codes that are linear in space and time," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 1804-1824, July 2002.
- [25] M. O. Damen, A. Tewfik, and J.-C. Belfiore, "A construction of a space-time code based on number theory," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 753-761, Mar. 2002.
- [26] K. P. Srinath and B. S. Rajan, "Generalized Silver Codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6134-6147, Sep. 2011.
- [27] N. Jacobson, *Basic Algebra II*. 2nd ed. New York: W.H. Freeman, 1985.
- [28] K. P. Srinath and B. S. Rajan, "Improved Perfect Space-Time Block Codes", available online at arXiv.